GFI Product Manual

GFI MailEssentials™

Administration and Configuration Manual

http://www.gfi.com

info@gfi.com

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.
If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.
All product and company names herein may be trademarks of their respective owners.
GFI MailEssentials is copyright of GFI SOFTWARE Ltd. - 1999-2011 GFI Software Ltd. All rights reserved.
Version ME-ACM-EN-1-02.010
Last updated: September 7, 2011

Contents

1 Introduction 7

1.1 Using this manual 7
1.2 Glossary of terms 7

2 About GFI MailEssentials 11

2.1 Minimum Requirements & Installation 11
2.2 How email processing works? 11
2.3 Description of anti-spam filters and actions 12
2.4 Licensing 14

3 Viewing anti-spam processing status 15

3.1 Using the GFI MailEssentials dashboard 15
3.2 Email Reports 17
3.3 Spam status reports 19

4 Routine Administration 29

4.1 Using Quarantine 29
4.2 Using Public folder scanning 33

5 Configuring anti-spam 35

5.1 Anti-spam filters 35
5.2 Spam Actions - What to do with spam email 64
5.3 Configuring Quarantine 68
5.4 Public folder scanning 72

6 Customizing other features 81

6.1 Disclaimers 81
6.2 Auto-replies 85
6.3 List servers 87
6.4 Email monitoring 94

7 Customizing GFI MailEssentials setup 99

7.1 Inbound email domains 99
7.2 Administrator email address 100
7.3 DNS server settings 100
7.4 SMTP Server settings 101
7.5 Automatic updates 102

8 Miscellaneous 105

8.1 Setting up POP3 and dialup downloading 105
8.2 Synchronizing configuration data 108
8.3 Exporting and importing GFI MailEssentials settings 113
8.4 Selecting the SMTP Virtual Server to bind GFI MailEssentials 116
8.5 Disabling/Enabling email processing 117
8.6 Tracing 118
8.7 Remote commands 119
8.8 Moving spam email to user's mailbox folders 124

9 Troubleshooting & support 129

9.1 Introduction 129
9.2 User manual 129
9.3 Common issues 129
9.4 Managing Spam 129
9.5 Archiving and Reporting 130
9.6 Anti-Spam filters & actions 131
9.7 Quarantine 132
9.8 Disclaimers 132
9.9 Email monitoring 132
9.10 List Server 132
9.11 Miscellaneous 133
9.12 Knowledge Base 133
9.13 Common checks 133
9.14 Web Forum 133
9.15 Request technical support 133
9.16 Build notifications 134
9.17 Documentation 134

10 Appendix - Bayesian Filtering **135**

Index **141**

List of screenshots

Screenshot 1 - GFI MailEssentials Dashboard: Status tab 15
Screenshot 2 - GFI MailEssentials Dashboard: Statistics tab 16
Screenshot 3 - Spam digest properties/Administrator spam digest 17
Screenshot 4 - Recipient spam digest 18
Screenshot 5 - Spam digest recipient list 19
Screenshot 6 - Daily spam report 20
Screenshot 7 - Anti-spam Rules Report 21
Screenshot 8 - User usage statistics filter dialog 22
Screenshot 9 - Domain usage statistics filter dialog 23
Screenshot 10 - Mail server daily usage statistics filter dialog 24
Screenshot 11 - The user communications report shows exact email trail 25
Screenshot 12 - User communications filter dialog 26
Screenshot 13 - Excluded users dialog 26
Screenshot 14 - The Quarantine Management page 30
Screenshot 15 - The Quarantine search 31
Screenshot 16 -Quarantine search results 32
Screenshot 17 - Previewing a quarantined email 32
Screenshot 18 - Quarantine email report 33
Screenshot 19 - SpamRazer Properties 36
Screenshot 20 - Automatic SpamRazer updates 37
Screenshot 21 - Phishing keywords 38
Screenshot 22 - Automatic anti-phishing updates 39
Screenshot 23 - The directory harvesting feature 40
Screenshot 24 - Anti-spam ordering dialog 42
Screenshot 25 - The email blocklist 43
Screenshot 26 - Adding more IP DNS Blocklists 44
Screenshot 27 - URI DNS Blocklist properties 45
Screenshot 28 - Configuring the SPF block level 47
Screenshot 29 - Configuring the SPF exceptions 48
Screenshot 30 - Greylist 49
Screenshot 31 - Email exclusions 50
Screenshot 32 - Adding email exclusions 50
Screenshot 33 - IP address exclusions 51
Screenshot 34 - Header checking general tab 52
Screenshot 35 - Language detection 53
Screenshot 36 - Anti-spam keyword checking properties 54
Screenshot 37 - Adding a condition 55
Screenshot 38 - Supplying ham to the Bayesian filter 56
Screenshot 39 - Bayesian analysis properties 57
Screenshot 40 - Whitelisted domains 58
Screenshot 41 - Auto Whitelist options 59
Screenshot 42 - Whitelisting keywords 60
Screenshot 43 - Whitelisting IPs 61
Screenshot 44 - New Senders properties 62
Screenshot 45 - New Senders Exception setup 63
Screenshot 46 - Assigning filter Priorities 64
Screenshot 47 - Configuring the action that should be taken 65
Screenshot 48 - The other actions tab 67
Screenshot 49 - Global actions 68
Screenshot 50 - Quarantine settings 69
Screenshot 51 - User settings 70
Screenshot 52 - Quarantine email schedule 70
Screenshot 53 - Selecting the users to receive the quarantine email reports 71
Screenshot 54 - Configuring advanced quarantine settings 72
Screenshot 55 - Configuring Public folder scanning 73
Screenshot 56 - Setting user role 75
Screenshot 57 - Selecting a domain or user disclaimer 81
Screenshot 58 - New disclaimer general properties 82
Screenshot 59 - HTML disclaimer 83
Screenshot 60 - The HTML disclaimer editor 83
Screenshot 61 - Plain text disclaimer 84

Screenshot 62 - Creating a new auto reply 85
Screenshot 63 - Auto-reply properties 86
Screenshot 64 - Variables dialog 86
Screenshot 65 - Creating a new newsletter list 88
Screenshot 66 - Specifying database backend 89
Screenshot 67 - Mapping custom fields 90
Screenshot 68 - Newsletter footer properties 91
Screenshot 69 - Setting permissions to the newsletter 92
Screenshot 70 - Entering subscribers to the newsletter 93
Screenshot 71 - Enable or disable email monitoring 95
Screenshot 72 - Add Mail Monitoring rule 95
Screenshot 73 - Configuring email monitoring 96
Screenshot 74 - Creating an exception 97
Screenshot 75 - Adding an inbound email domain 99
Screenshot 76 - Administrator email address 100
Screenshot 77 - DNS server settings 101
Screenshot 78 - Perimeter SMTP Server settings 102
Screenshot 79 - Configuring automatic updates 103
Screenshot 80 - The GFI MailEssentials pop3 downloader 105
Screenshot 81 - Adding a POP3 mailbox 106
Screenshot 82 - Dial-up options 107
Screenshot 83 - Configuring when GFI MailEssentials should pick up email 108
Screenshot 84 - Configuring a master server 110
Screenshot 85 - Configuring a slave server 112
Screenshot 86 - Upload / download hourly interval setting 112
Screenshot 87 - GFI MailEssentials Configuration Export/Import Tool 113
Screenshot 88 - Exporting settings via command line 114
Screenshot 89 - Importing settings via command line 116
Screenshot 90 - SMTP Virtual Server Bindings 117
Screenshot 91 - The GFI MailEssentials Switchboard: Troubleshooting 118
Screenshot 92 - Tracing 119
Screenshot 93 - Remote commands configuration 120
Screenshot 94 - Adding an email address to the blocklist and keywords 122
Screenshot 95 - Specifying the same commands more than once 122
Screenshot 96 - Adding spam to the Bayesian filter database 123
Screenshot 97 - Sending remote commands without security 123
Screenshot 98 - The GFI MailEssentials Rules Manager 125
Screenshot 99 - Adding a new rule in Rules Manager 125
Screenshot 100 - List of rules in Rules Manager 126
Screenshot 101 - Select the Bayesian spam profile to update 137
Screenshot 102 - Select the legitimate email source 138
Screenshot 103 - Select the spam source 139

1 Introduction

GFI MailEssentials is a server-based anti-spam solution that provides key corporate email anti-spam features for your mail server. Installed as an add-on to your mail server, GFI MailEssentials is completely transparent to users, with no additional user training required.

The key features of this solution are:

- **Server-based anti-spam** - Spam protection is an essential component of your network's security strategy. GFI MailEssentials offers advanced anti-spam filters which include blocklist/whitelist, Bayesian filtering, keyword checking, and header analysis.
- **Quarantine** - incoming spam emails are retained in a central store for a number of days. This simplifies management of emails and reduces processing on the mail server.
- **Company-wide disclaimer/footer text -** Companies are responsible for the content of their employees' email messages. GFI MailEssentials enables the automatic addition of disclaimers on top or the bottom of an email, together with fields/variables that personalize the disclaimer according to the recipient.
- **Reporting -** GFI MailEssentials can produce various useful reports on email usage and anti spam operations.
- **Personalized auto-replies with tracking number** - More than just an 'out of office' replies, auto-replies enable customers to know that their email has been received and that their request is being handled. Assign a unique tracking number to each reply to give your customers and employees an easy point of reference.
- **POP3 downloader -** Smaller businesses may not have the necessary facilities to use SMTP based email. GFI MailEssentials includes a utility that can forward and distribute email from POP3 mailboxes to mailboxes on the mail server.
- **Email monitoring -** Central information stores are typically easier to manage than distributed information. GFI MailEssentials enables sending of email copies to a central store of email communications of a particular person or department.

For more information how GFI MailEssentials filters emails for inbound and outbound emails, refer to **About GFI MailEssentials** in this manual.

1.1 Using this manual

This user manual is a comprehensive guide that aims to assist systems administrators in configuring and using GFI MailEssentials in the best way possible. It builds up on the instructions provided in the GFI MailEssentials 'Getting Start Guide' and describes the configuration settings that systems administrators must do so to achieve the best possible results out of the software

1.2 Glossary of terms

A list of terms used in this manual and a brief definition.

Active Directory	A technology that provides a variety of network services, including LDAP-like directory services.
AD	*See* Active Directory
Auto-reply	An email reply that is sent automatically to incoming emails.
Bayesian Filtering	An anti-spam technique where a statistical probability index based on training from users is used to identify spam.
Background Intelligent Transfer Service	A component of Microsoft Windows operating systems that facilitates transfer of files between systems using idle network bandwidth.
BITS	*See* Background Intelligent Transfer Service

Blocklist	A list of email addresses or domains from whom email is not to be received by users
Botnet	A network of infected computers that run autonomously and are controlled by a hacker/cracker.
CIDR	*See* Classless Inter-Domain Routing
Classless Inter-Domain Routing	An IP addressing notation that defines a range of IP addresses.
Demilitarized Zone	A section of a network that is not part of the internal network and is not directly part of the Internet. Its purpose typically is to act as a gateway between internal networks and the internet.
Disclaimer	A statement intended to identify or limit the range of rights and obligations for email recipients
Domain Name System	A database used by TCP/IP networks that enables the translation of hostnames into IP numbers and to provide other domain related information.
DMZ	*See* Demilitarized Zone
DNS	*See* Domain Name System
DNS MX	*See* Mail Exchange
Email monitoring rules	Rules which enable the replication of emails between email addresses.
False negatives	Spam emails that are not detected as spam.
False positives	Legitimate emails that are incorrectly identified as spam.
Greylist filter	An anti-spam filter that blocks emails sent from spammers that do not resend a message when a retry message is received.
Ham	Legitimate e-mail
IIS	*See* Internet Information Services
Internet Information Services	A set of Internet-based services created by Microsoft Corporation for internet servers.
IMAP	*See* Internet Message Access Protocol
Internet Message Access Protocol	One of the two most commonly used Internet standard protocols for e-mail retrieval, the other being POP3.
LDAP	*See* Lightweight Directory Access Protocol
Lightweight Directory Access Protocol	An application protocol used to query and modify directory services running over TCP/IP
List server	A server that distributes emails sent to discussions lists and newsletter lists, and manages subscription requests.
Mail Exchange	The DNS record used to identify the IP addresses of the domain's mail servers.
MAPI	*See* Messaging Application Programming Interface
MDAC	*See* Microsoft Data Access Components
Messaging Application Programming Interface	A messaging architecture and a Component Object Model based API for Microsoft Exchange.
Microsoft Message Queuing Services	A message queue implementation for Windows Server operating systems.
Microsoft Data Access Components	A Microsoft technology that gives developers a homogeneous and consistent way of developing software that can access almost any data store.

MIME	*See* Multipurpose Internet Mail Extensions
MSMQ	*See* Microsoft Message Queuing Services
Multipurpose Internet Mail Extensions	A standard that extends the format of e-mail to support text other than ASCII, non-text attachments, message bodies with multiple parts and header information in non-ASCII character sets.
NDR	*See* Non Delivery Report
Non Delivery Report	An automated electronic mail message sent to the sender on an email delivery problem.
Perimeter server/gateway	The computer (server) in a LAN that is directly connected to an external network. In GFI MailEssentials perimeter gateway refers to the email servers within the company that first receive email from external domains.
Phishing	The process of acquiring sensitive personal information with the aim of defrauding individuals, typically through the use of fake communications
POP2Exchange	A system that collects email messages from POP3 mailboxes and routes them to mail server.
POP3	*See* Post Office Protocol ver.3
Post Office Protocol ver.3	A protocol used by local email clients to retrieve emails from mailboxes over a TCP/IP connection.
Public folder	A common folder that allows Microsoft Exchange user to share information.
Quarantine	A database where all inbound emails detected as spam are retained for a number of days
RBL	*See* Realtime Blocklist
Realtime Blocklist	Online databases of spam IP addresses. Incoming emails are compared to these lists to determine if they are originating from blocked users.
Remote commands	Instructions that facilitate the possibility of executing tasks remotely.
Secure Sockets Layer	A protocol to ensure an integral and secure communication between networks.
Simple Mail Transport Protocol	An internet standard used for email transmission across IP networks.
SMTP	*See* Simple Mail Transport Protocol
Spam actions	Actions taken on spam emails received, e.g. delete email or send to Junk email folder.
SSL	*See* Secure Sockets Layer
WebDAV	A HTTP extensions database that enables users to manage files remotely and interactively. Used for managing emails in the mailbox and in the public folder in Microsoft Exchange.
Whitelist	A list of email addresses and domains from which emails are always received
Zombie	An infected computer that is part of a Botnet.

2 About GFI MailEssentials

2.1 Minimum Requirements & Installation

For information on system requirements and installation refer to the GFI MailEssentials 'Getting Started Guide':

http://www.gfi.com/mes/manual

2.2 How email processing works?

2.2.1 Inbound mail filtering

Inbound mail filtering is the process through which incoming email are filtered before delivery to users.

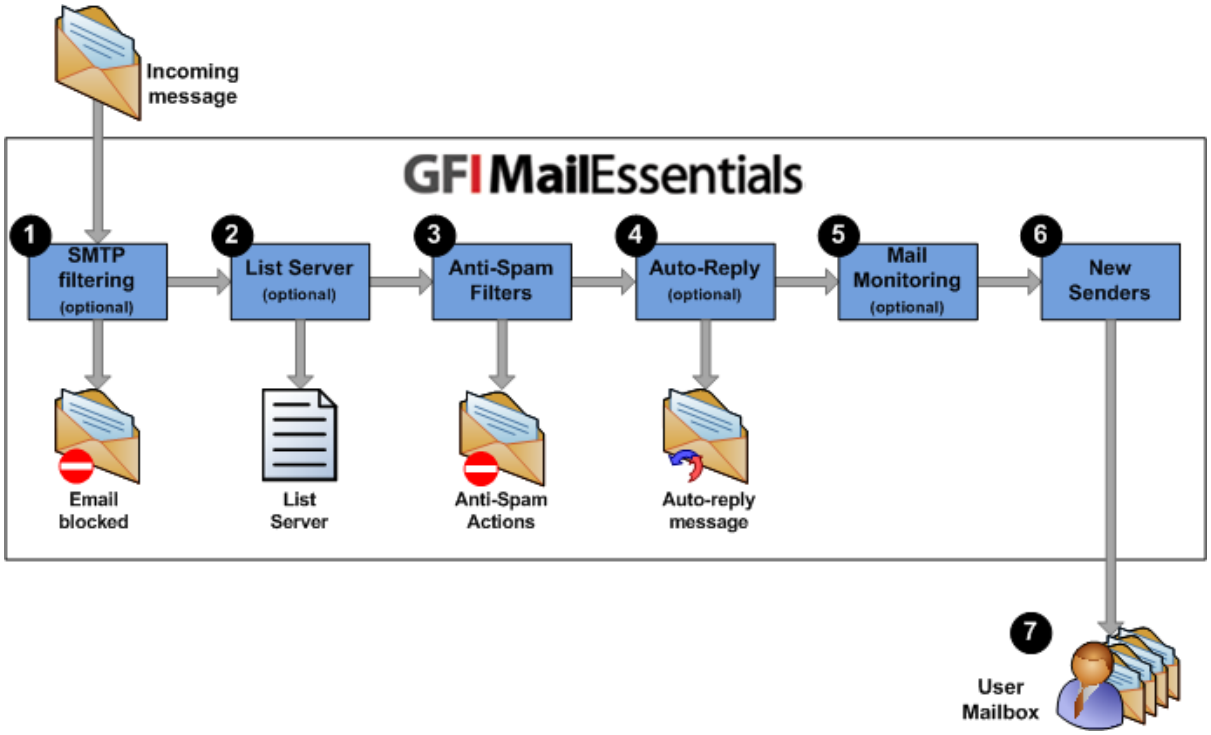


Figure 1 - Inbound mail filtering

When an email is received:

1. SMTP level filtering (Directory Harvesting and Greylist) is executed before the email body is received.

2. When the email is received, it is checked to see if it is addressed to a list in the list server. If the email matches a list, it will be processed by the list server.

3. The incoming email is filtered using all the spam filters. Any email that fails a spam filter check is sent to the anti spam email actions. If an email goes through all the filters and is not identified as spam, it then goes to the next stage.

4. If configured, auto-replies are next sent to the sender.

5. If configured, email monitoring is next executed and the appropriate actions taken.

6. The new senders filter is now executed.

7. Email is sent to the user's mailbox.

2.2.2 Outbound mail filtering

Outbound mail filtering is the process through which email sent by users within a company is processed before it is sent out.

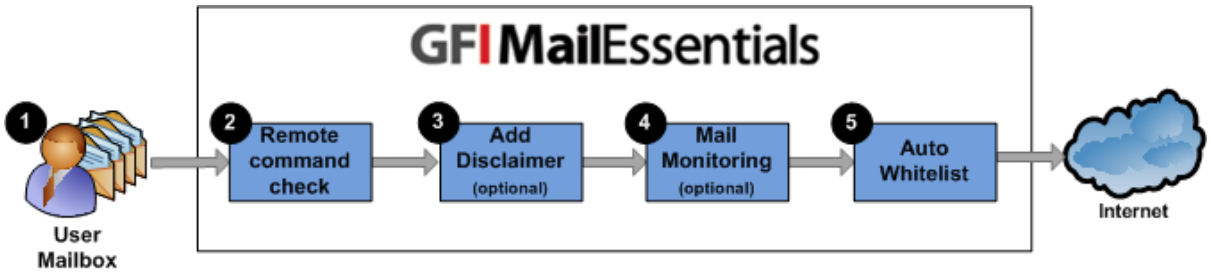


Figure 2 - Outbound mail filtering

1 User creates and sends email.

2 Remote commands check executes any remote commands in email if any are found. If none are found, email goes to the next stage.

3 If configured, the applicable disclaimer is next added to the email.

4 Email is checked for any mail monitoring which may apply and action is taken according to any rules configured.

5 If enabled, auto-whitelist adds the recipient's email address to the whitelist. This automatically enables replies from such recipients to go to the sender without being checked for spam. After this check, the email is sent to the recipients.

2.3 Description of anti-spam filters and actions

About anti-spam filters

Out of the box, GFI MailEssentials includes a number of specialized anti-spam filters. Each one of these filters target one or more types of spam. The filters included with GFI MailEssentials are listed below:

FILTER	DESCRIPTION	ENABLED BY DEFAULT
SpamRazer	An anti-spam engine that determines if an email is spam by using email reputation, message fingerprinting and content analysis.	Yes
Directory Harvesting	Stops email which is randomly generated towards a server, mostly addressed to non-existent users.	No
Phishing	Blocks emails that contain links in the message bodies pointing to known phishing sites or if they contain typical phishing keywords.	Yes
Sender Policy Framework	Stops email which is received from domains not authorized in SPF records	No
Auto-Whitelist	Addresses to which an email is sent to, are automatically excluded from being blocked.	Yes
Whitelist	A custom list of safe email addresses	Yes
Email Blocklist	A custom list of blocked email users or domains.	Yes
IP DNS Blocklist	Checks if the email received is from senders that are listed on a public DNS list of known spammers.	Yes
URI DNS Blocklist	Stops emails which contain links to domains listed on public Spam URI Blocklists	Yes

FILTER	DESCRIPTION	ENABLED BY DEFAULT
Header checking	A module which detects spam by analyzing the email header.	Yes
Keyword checking	Spam messages are identified based on blocked keywords in the email subject or body	Yes
New Senders	Emails that have been received from senders to whom emails have never been sent before.	No
Bayesian analysis	An anti-spam technique where a statistical probability index based on training from users is used to identify spam.	No
Greylist	Identifies emails received from Non RFC compliant mail servers such as the ones normally used by spammers.	No

As listed in the table above, not all anti-spam filters are enabled by default. This is due to configuration settings which are network/infrastructure dependent and cannot therefore be preset. Although key filters like SpamRazer are enabled by default, it is recommended that after installing GFI MailEssentials, the rest of the anti-spam filters and filtering mechanisms are reviewed and enabled accordingly. For more information refer to the **Anti-spam filters** chapter in this manual.

Anti-Spam actions

A number of actions can be triggered by anti-spam filters on detection of spam email. These actions determine what will happen to emails detected as spam and are configurable on a filter by filter basis. Anti-spam filter actions supported are:

- Delete spam.
- Quarantine email (recommended action)
- Move email spam to a mailbox folder
- Forward email spam to a specific email address
- Save email spam to a folder on disk
- Tag spam email
- Move email spam to a central folder
- Forward email spam to mail-enabled public folders

For more information about anti-spam actions refer to the **Spam Actions - What to do with spam email** section in this manual.

Default Anti-Spam actions

The default action taken when GFI MailEssentials blocks a spam email is chosen during the post-install wizard. If the post-install wizard is skipped, the default action taken when GFI MailEssentials blocks a spam email depends where the software is installed:

DEPLOYMENT	DEFAULT ACTION	DESCRIPTION
GFI MailEssentials installed on the same computer as Microsoft Exchange	Deliver email in Exchange mailbox sub-folder	When a filter blocks a spam email, the email is moved to a sub-folder in Inbox named Suspected Spam.
GFI MailEssentials not installed on the same machine as Microsoft Exchange	Tagging	Anti-spam filters adding the prefix [SPAM] in the subject field of spam emails. Tagged emails are still delivered in the user's Inbox.

For more information about anti-spam actions refer to the **Spam Actions - What to do with spam email** section in this manual.

2.4 Licensing

For information on licensing refer to:
http://www.gfi.com/products/gfi-mailessentials/pricing/licensing

3 Viewing anti-spam processing status

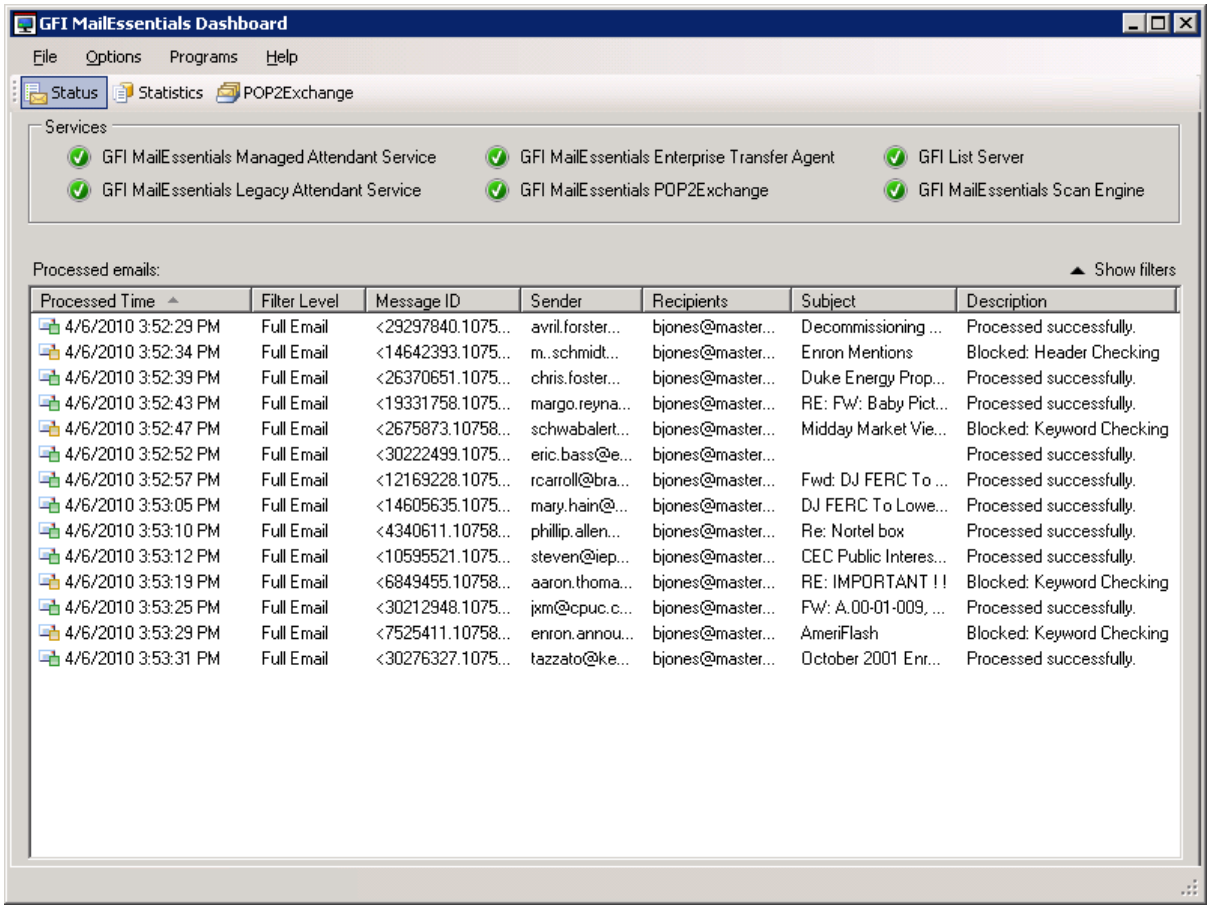
3.1 Using the GFI MailEssentials dashboard

The GFI MailEssentials Dashboard shows the status of your anti-spam system, including email processing activity and statistics.

3.1.1 Monitoring the status in real-time

From the Status tab within the GFI MailEssentials Dashboard, you can monitor the GFI MailEssentials services and email processing activity in real-time.

1. Click **Start ► All Programs ► GFI MailEssentials ► GFI MailEssentials Dashboard.**


GFI MailEssentials Dashboard
File
Options
Programs
Help
Status
Statistics
POP2Exchange
Services
GFI MailEssentials Managed Attendant Service
GFI MailEssentials Enterprise Transfer Agent
GFI List Server
GFI MailEssentials Legacy Attendant Service
GFI MailEssentials POP2Exchange
GFI MailEssentials Scan Engine
Processed emails:
Show filters
Processed Time | Filter Level | Message ID | Sender | Recipients | Subject | Description
4/6/2010 3:52:29 PM | Full Email | <29297840.1075... | avril.forster... | bjones@master... | Decommissioning ... | Processed successfully.
4/6/2010 3:52:34 PM | Full Email | <14642393.1075... | m..schmidt... | bjones@master... | Enron Mentions | Blocked: Header Checking
4/6/2010 3:52:39 PM | Full Email | <26370651.1075... | chris.foster... | bjones@master... | Duke Energy Prop... | Processed successfully.
4/6/2010 3:52:43 PM | Full Email | <19331758.1075... | margo.reyna... | bjones@master... | RE: FW: Baby Pict... | Processed successfully.
4/6/2010 3:52:47 PM | Full Email | <2675873.10758... | schwabalert... | bjones@master... | Midday Market Vie... | Blocked: Keyword Checking
4/6/2010 3:52:52 PM | Full Email | <30222499.1075... | eric.bass@e... | bjones@master... | | Processed successfully.
4/6/2010 3:52:57 PM | Full Email | <12169228.1075... | rcarroll@bra... | bjones@master... | Fwd: DJ FERC To ... | Processed successfully.
4/6/2010 3:53:05 PM | Full Email | <14605635.1075... | mary.hain@... | bjones@master... | DJ FERC To Lowe... | Processed successfully.
4/6/2010 3:53:10 PM | Full Email | <4340611.10758... | phillip.allen... | bjones@master... | Re: Nortel box | Processed successfully.
4/6/2010 3:53:12 PM | Full Email | <10595521.1075... | steven@iep... | bjones@master... | CEC Public Interes... | Processed successfully.
4/6/2010 3:53:19 PM | Full Email | <6849455.10758... | aaron.thoma... | bjones@master... | RE: IMPORTANT ! ! | Blocked: Keyword Checking
4/6/2010 3:53:25 PM | Full Email | <30212948.1075... | jxm@cpuc.c... | bjones@master... | FW: A.00-01-009, ... | Processed successfully.
4/6/2010 3:53:29 PM | Full Email | <7525411.10758... | enron.annou... | bjones@master... | AmeriFlash | Blocked: Keyword Checking
4/6/2010 3:53:31 PM | Full Email | <30276327.1075... | tazzato@ke... | bjones@master... | October 2001 Enr... | Processed successfully.

Screenshot 1 - GFI MailEssentials Dashboard: Status tab

2. Select **Status** tab.

The **Services** area shows the status of the GFI MailEssentials services. All services need to be on for correct operation of the software.

The **Processed emails** area lists the emails processed by GFI MailEssentials and a description of the status of the email. You can also filter the list of processed emails by clicking **Show filters**. Key in the criteria to search for and matching entries are displayed in the list. You can search by:

- Subject
- Message ID
- Sender
- Recipient

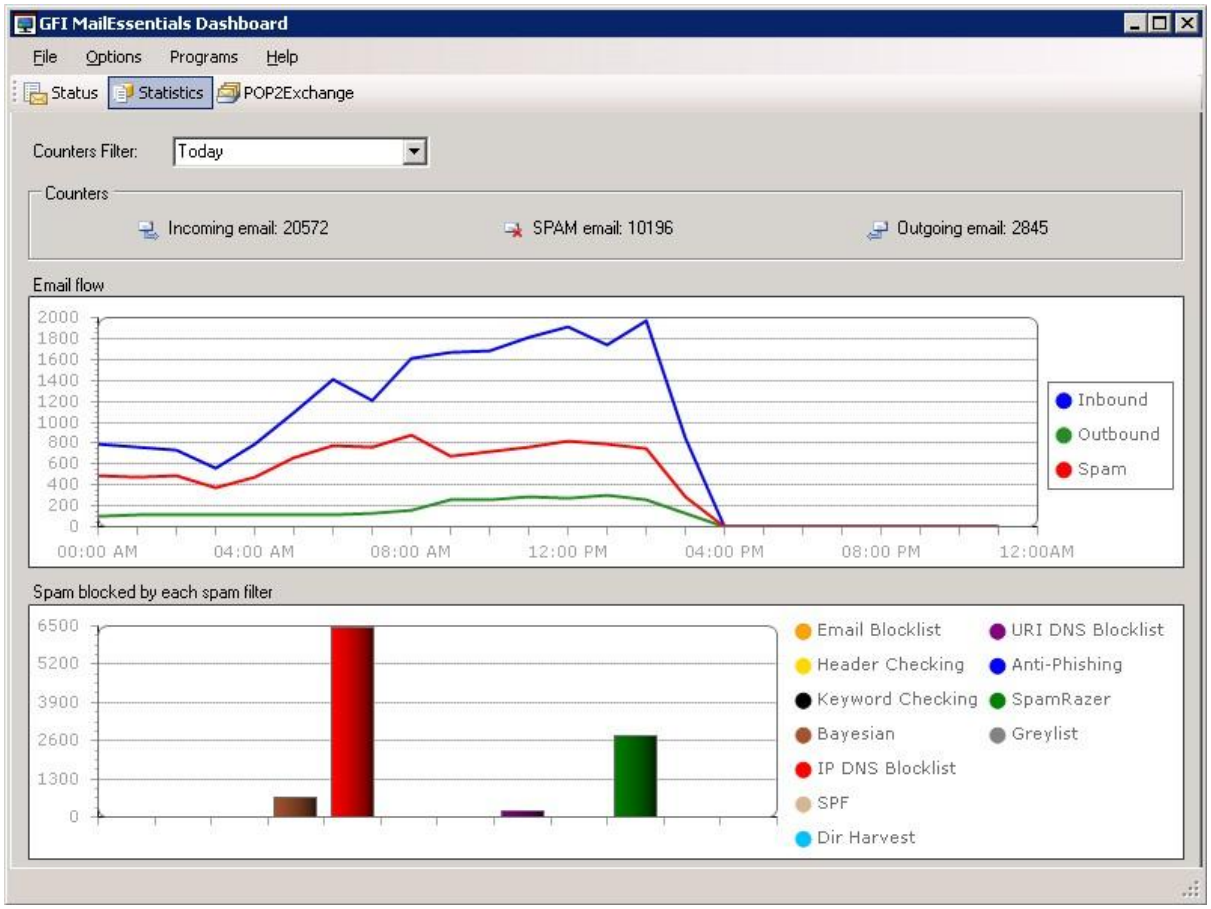
The list can be further filtered by type and description of the email. Navigate to **Options ► Email Log Filter** and select to display email with any of the following options:

- **Delivered email** - emails allowed delivery to their intended recipients.
- **Blocked email** - emails blocked by any of the anti-spam filters.
- **Whitelisted email** - emails that match a whitelist entry and that were delivered to their intended recipients without further scanning.
- **Failed email** - emails that failed email scanning or failed delivery. Email is stored in the **FailedMails** folder within the GFI MailEssentials installation folder.
- **Inbound email** - incoming emails that are addressed to local users.
- **Outbound email** - outgoing emails sent by local users to external users.

NOTE: Navigate to **Options ► Select Columns** to select the columns to display in the Processed emails list.

3.1.2 Statistics

From the Statistics tab of the GFI MailEssentials Dashboard, you can view statistical information related to email scanning.



Screenshot 2 - GFI MailEssentials Dashboard: Statistics tab

- **Counters Filter** - specify the period to view statistics for.
- **Counters** - displays the number of incoming and outgoing email, and the number of emails identified as spam.
- **Email flow** - a time chart showing the number of inbound, outbound and spam emails processed during every hour or day, depending on the period selected.
- **Spam blocked by each spam filter** - shows the number of emails blocked by each spam filter.

3.1.3 POP2Exchange

The POP2Exchange tab of the GFI MailEssentials Dashboard, shows a log of the POP2Exchange

activities.

NOTE: For information on POP2Exchange refer to the **Setting up POP3 and dialup downloading** section in this manual.

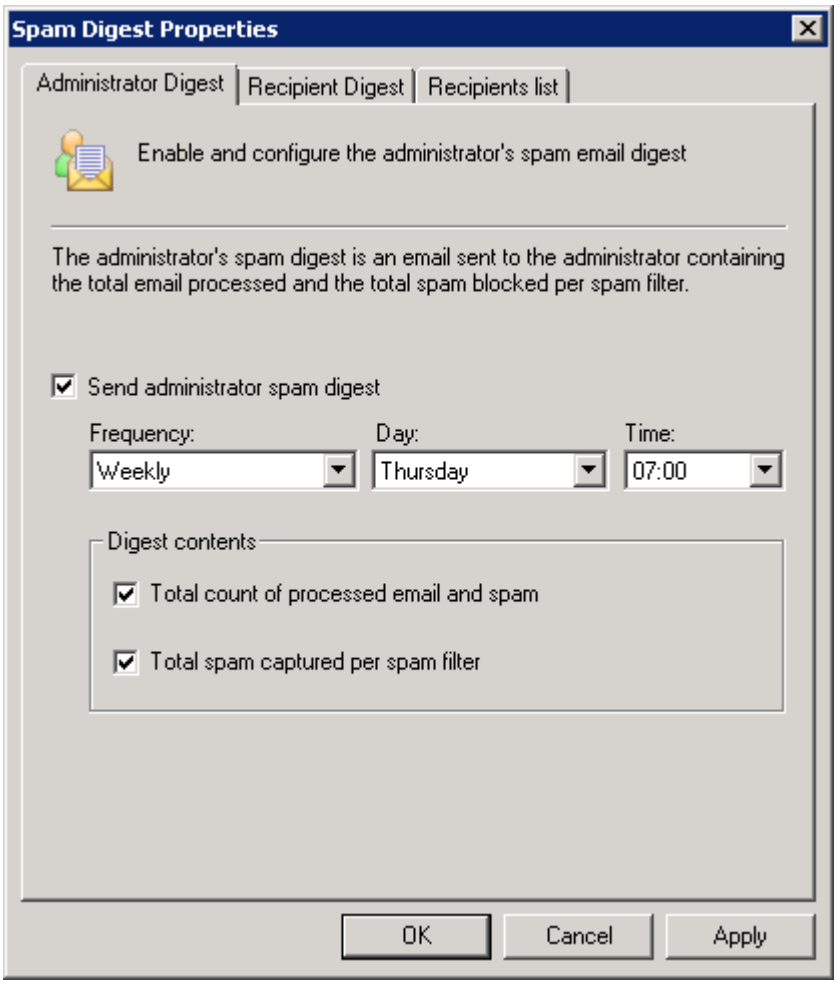
3.2 Email Reports

The spam digest is a short report sent to an administrator or user via email. This report lists the total number of emails processed by GFI MailEssentials and the number of spam emails blocked over a specific period of time (since the last spam digest).

3.2.1 Configuring spam digests

Administrator spam digest

1. Select **Anti-Spam ► Spam Digest ► Properties**.



Screenshot 3 - Spam digest properties/Administrator spam digest

2. From the **Administrator Digest** tab, click **Send administrator spam digest** to enable spam digest.

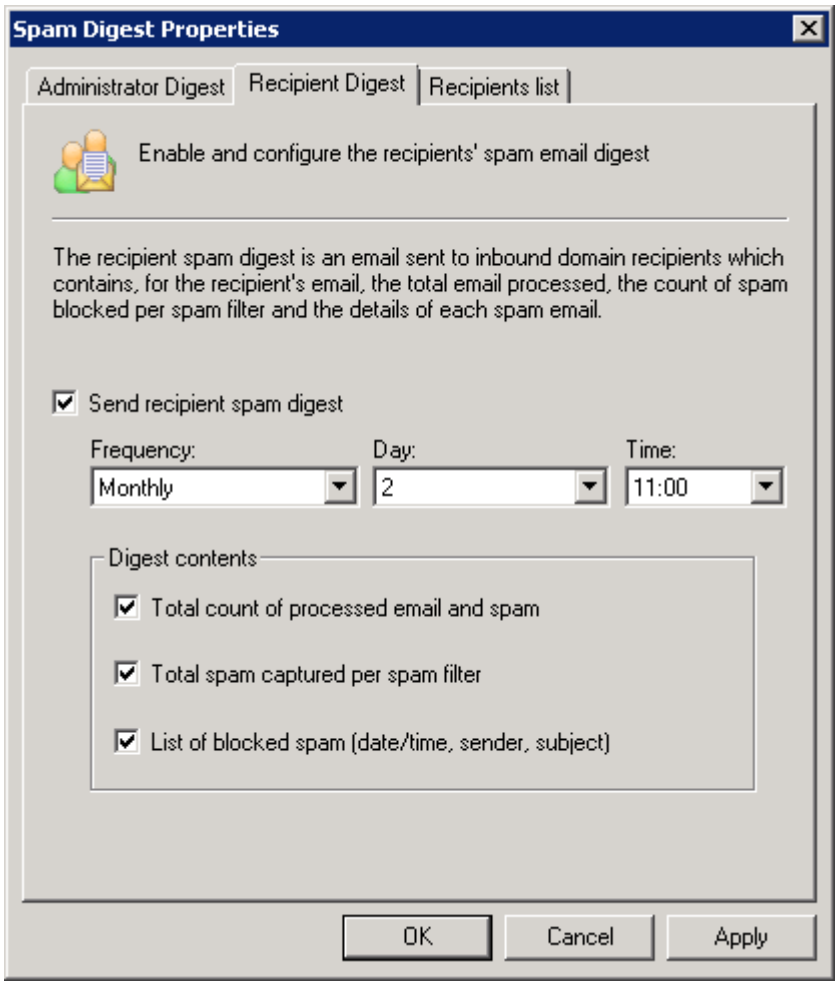
3. Configure the desired sending frequency (Daily, Weekly, Monthly) from the **Sending schedule** drop-down.

4. Specify the digest content that will be sent in the email, either a **Total count of processed email and spam** or **Total spam captured per spam filter** or both.

5. Finalize settings by selecting **Apply** and **OK**.

Recipient spam digest

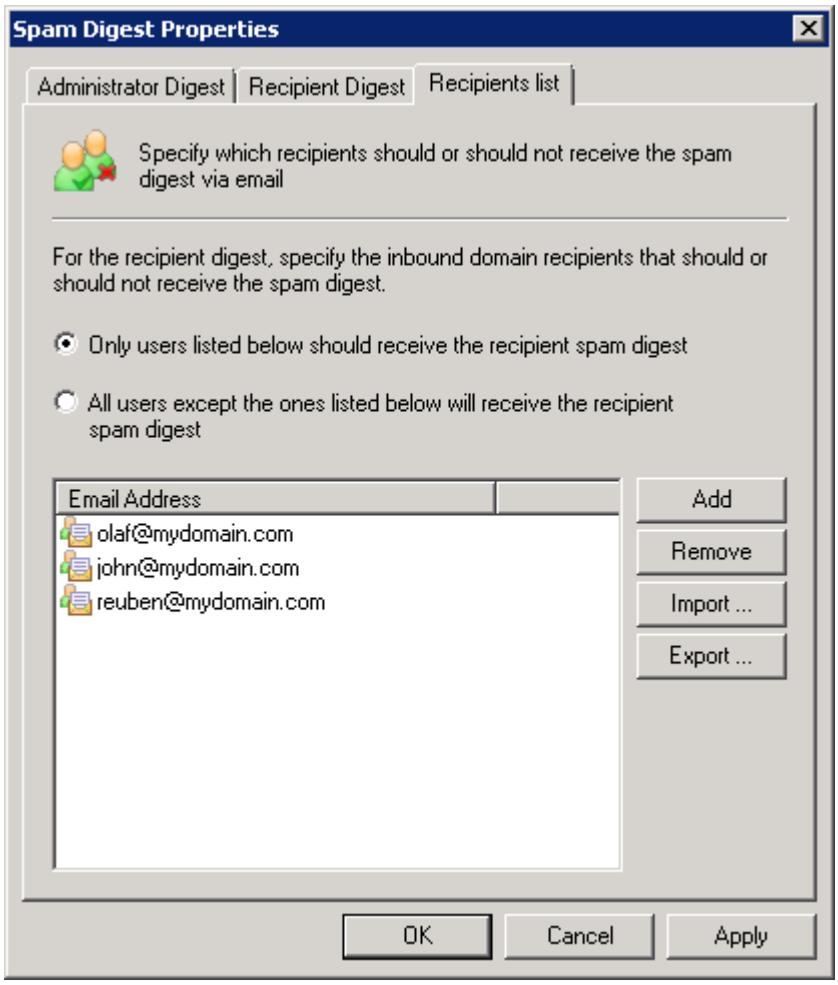
1. Select **Anti-Spam ► Spam Digest ► Properties**.


Spam Digest Properties
Administrator Digest
Recipient Digest
Recipients list
Enable and configure the recipients' spam email digest
The recipient spam digest is an email sent to inbound domain recipients which contains, for the recipient's email, the total email processed, the count of spam blocked per spam filter and the details of each spam email.
Send recipient spam digest
Frequency:
Monthly
Day:
2
Time:
11:00
Digest contents
Total count of processed email and spam
Total spam captured per spam filter
List of blocked spam (date/time, sender, subject)
OK
Cancel
Apply

Screenshot 4 - Recipient spam digest

2. From the **Recipient Digest** tab, select **Spam recipient spam digest** to enable spam digest.
3. Configure the desired sending frequency from **Sending schedule**.
4. Specify the digest content that will be sent in the email:
   - » Total count of processed email and spam
   - » Total spam captured per spam filter
   - » List of blocked spam

or any combination of options as required.


Spam Digest Properties
Administrator Digest
Recipient Digest
Recipients list
Specify which recipients should or should not receive the spam digest via email
For the recipient digest, specify the inbound domain recipients that should or should not receive the spam digest.
Only users listed below should receive the recipient spam digest
All users except the ones listed below will receive the recipient spam digest
Email Address
olaf@mydomain.com
john@mydomain.com
reuben@mydomain.com
Add
Remove
Import ...
Export ...
OK
Cancel
Apply

Screenshot 5 - Spam digest recipient list

5. Click on the **Recipients** list tab, add the users to receive the spam digest and select the method used to determine who should receive the spam digest. Available options are:

- Only users listed below should receive the recipient spam digest.
- All users except the ones listed below will receive the recipient spam digest.

NOTE: The required list of users can also be imported from a file in XML format in the same structure that GFI MailEssentials would export files.

6. Select **Apply** and **OK** to finalize settings.

3.3 Spam status reports

GFI MailEssentials enables you to create reports based on data logged to database. These reports assist you in knowing what spam is being filtered out by GFI MailEssentials and what are the use levels of your mail server and domain resources.

3.3.1 Enabling reporting

1. Select **Email Management ► Reporting ► Properties** and click **Configure** button.
2. Select database type:

- **Microsoft Access** - Specify the file name and location.
- **Microsoft SQL server** - Specify server name, logon credentials and database.

3. Click **Test** button to test the database configuration. Click **OK** to save settings.

Configuring database auto-purging

You can configure GFI MailEssentials to automatically delete (auto-purge) records from the

database that are older than a particular period. To enable auto-purging:

1. Navigate to **Email Management ► Reporting ► Properties** and select **Auto-purge** tab.

2. Select **Purge entries older than** and specify the auto-purging period in months.

NOTE: Auto-purging is applied only to the current database configured in the **Reporting** tab.

3. Click **OK** to save settings.

3.3.2 Using Reports

1. Launch the GFI MailEssentials Reporter by clicking **Start ► All Programs ► GFI MailEssentials ► GFI MailEssentials Reports**.

2. Click **Reports** Option and select any Report or Statistics option.

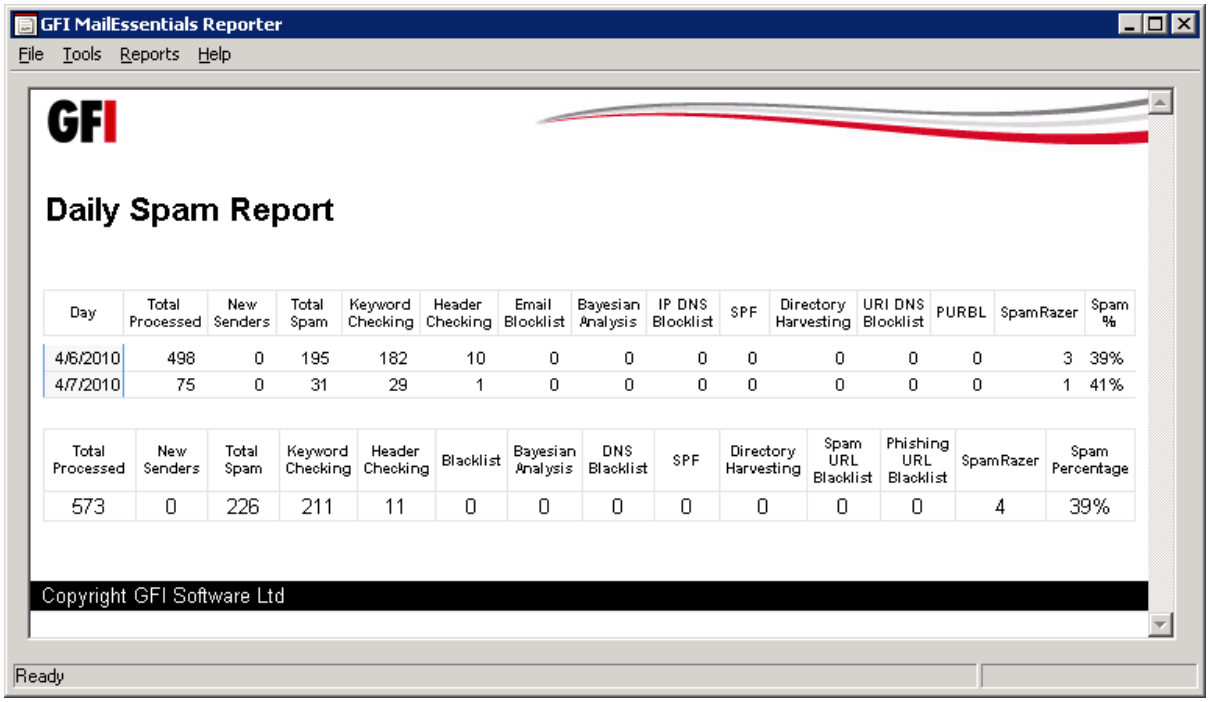
3. Specify report criteria and click **Report** to generate the report.

4. Reports can be saved in HTML format or printed.

NOTE: When saving the report in HTML format, two sub-folders are created, 'graphics' and 'report'. The 'report' sub-folder contains the report files in HTML format. The 'graphics' sub-folder contains graphics which are displayed in the HTML report.

3.3.3 Daily Spam Report

The Daily Spam Report shows the total emails processed, total spam email caught, the spam percentage of total emails processed and how many spam emails were caught by each individual anti-spam feature. Each row in the report represents a day.


GFI MailEssentials Reporter
File Tools Reports Help
GFI
Daily Spam Report
Day | Total Processed | New Senders | Total Spam | Keyword Checking | Header Checking | Email Blocklist | Bayesian Analysis | IP DNS Blocklist | SPF | Directory Harvesting | URI DNS Blocklist | PURBL | SpamRazer | Spam %
4/6/2010 | 498 | 0 | 195 | 182 | 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 39%
4/7/2010 | 75 | 0 | 31 | 29 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 41%
Total Processed | New Senders | Total Spam | Keyword Checking | Header Checking | Blacklist | Bayesian Analysis | DNS Blacklist | SPF | Directory Harvesting | Spam URL Blacklist | Phishing URL Blacklist | SpamRazer | Spam Percentage
573 | 0 | 226 | 211 | 11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 39%
Copyright GFI Software Ltd
Ready

Screenshot 6 - Daily spam report

Report Options

- **Sort column:** Sort the report by date, total spam processed, keyword checking etc.
- **Multi Page report:** Specify the number of days per page.

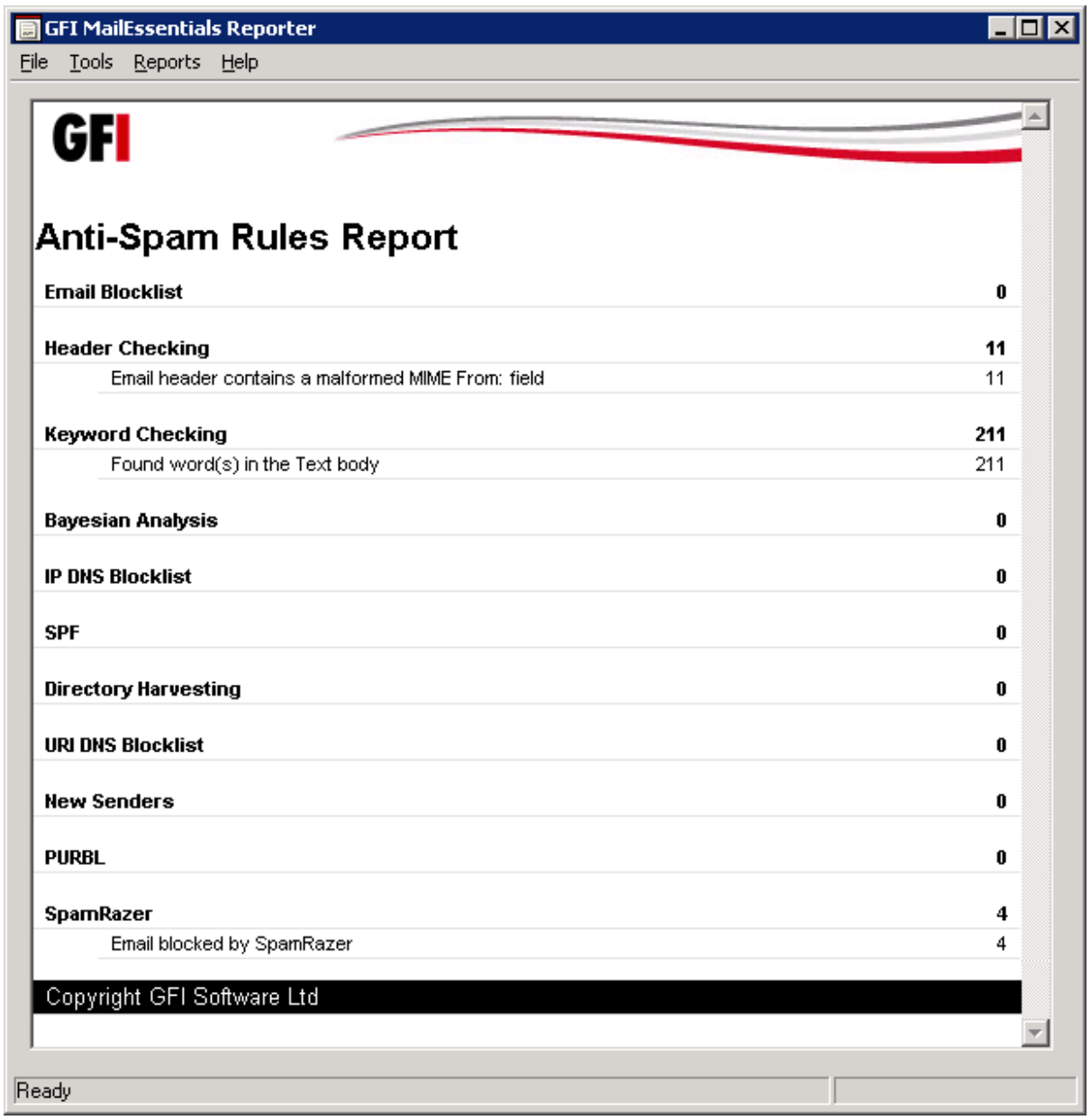
Filter options

- **Specific Email:** Limit report to a specific email address.
- **Date Range:** Limit report to a specific date range.

When all report options are selected, click **Report** to generate report.

3.3.4 Anti-Spam Rules Report

The Anti-spam Rules Report shows how much spam email each anti-spam method caught.



Screenshot 7 - Anti-spam Rules Report

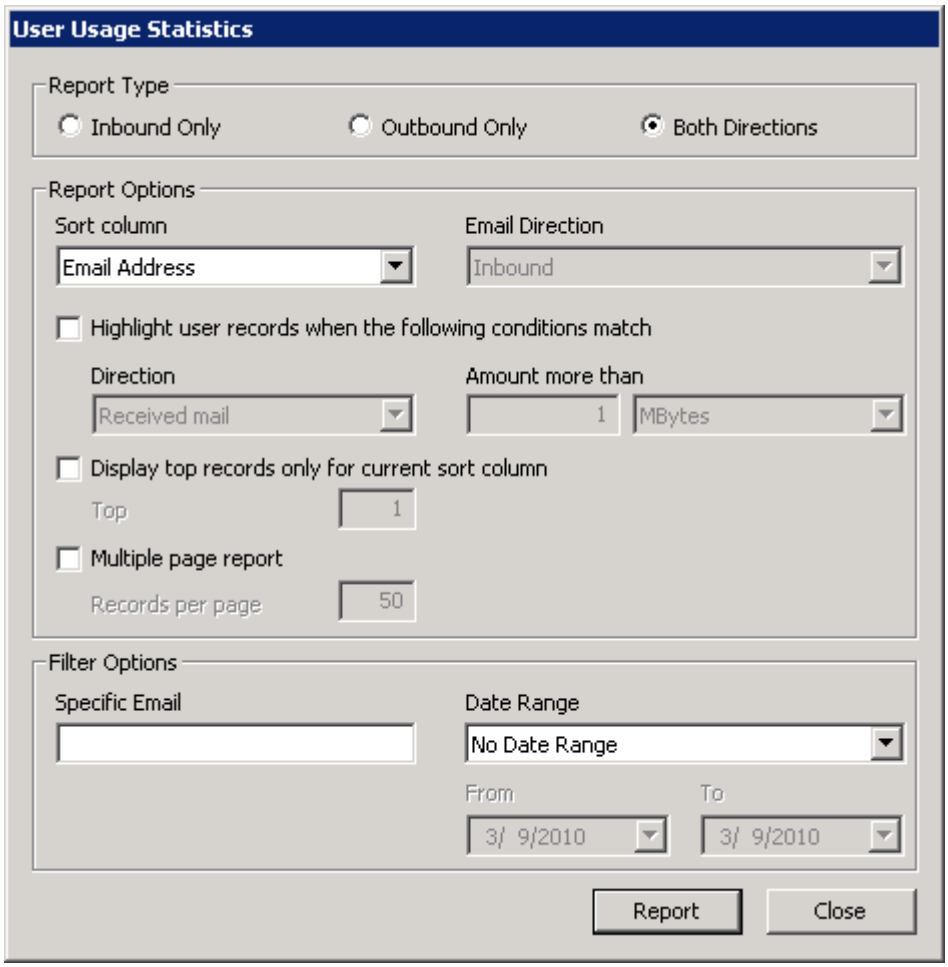
Report Options

- **Specific Email:** Limits the report to a specific email address.
- **Date Range:** Limits the report to a specific date range.

When all report options are selected, click **Report** button to generate report.

3.3.5 User Usage Statistics

The user usage statistics report gives an overview of how many emails users send or receive and how large their sent or received emails are.



Screenshot 8 - User usage statistics filter dialog

Report Type

- **Report Type:** Specify reporting on inbound emails, outbound emails, or both.

Report Options

- **Sort by:** Specify sorting by email address, by number of emails, or by the total size of the emails.
- **Highlight users:** Identify users who send or receive more than a specific number of emails or specific number of megabytes of email.
- **List top:** List only the top number of users in the report.
- **Multi Page report:** Specify the number of users to display per page.

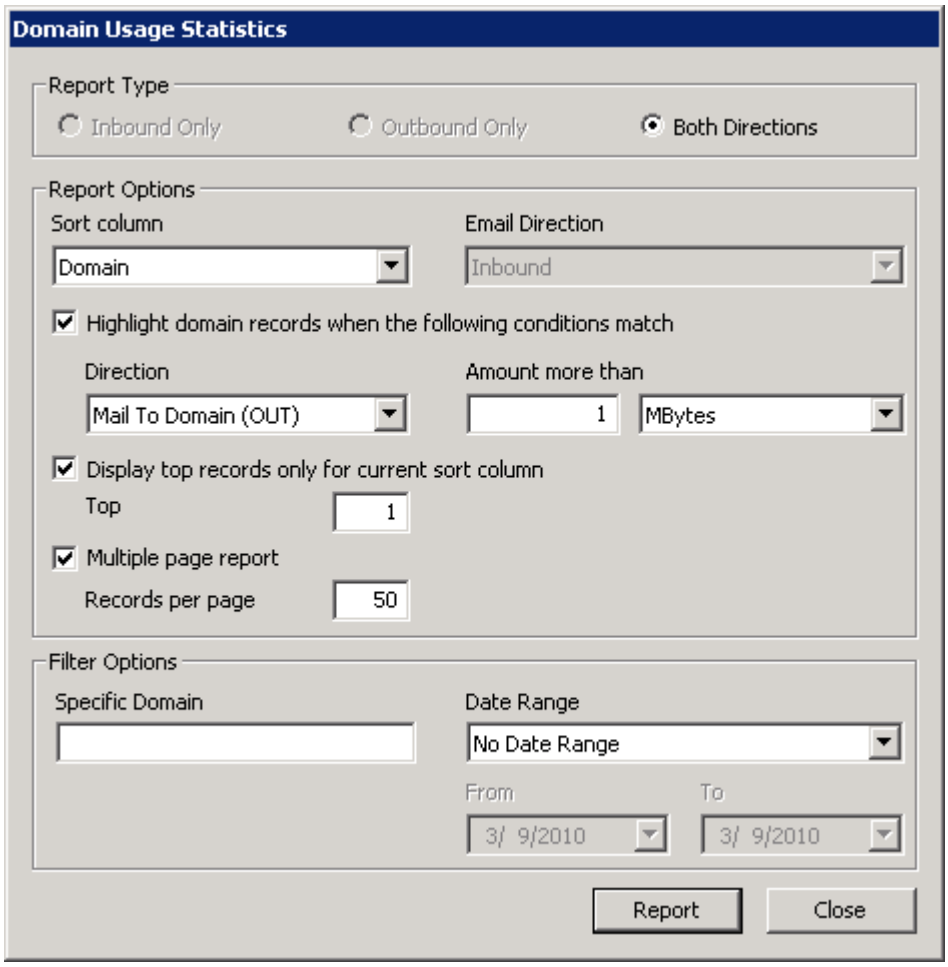
Filter options

- **Specific Email:** Limit the report to a specific email address.
- **Date Range**: Limit the report to a specific date range.

When all report options are selected, click **Report** button to generate report.

3.3.6 Domain Usage Statistics

The domain usage statistics report gives an overview of how many emails are sent or received to non-local domains.



Screenshot 9 - Domain usage statistics filter dialog

Report Type

- **Report Type:** By default report data for domain usage statistics is always for both inbound and outbound emails.

Report Options

- **Sort by:** Specify if the report is sorted by domain name, by number of emails, or by the total size of the emails.
- **Highlight domains:** Identify domains that send or receive more than a specific number of emails or a specific number of megabytes of email.
- **List to:** List only the top number of domains in the report.
- **Multi Page report:** Specify the number of domains to display per page.

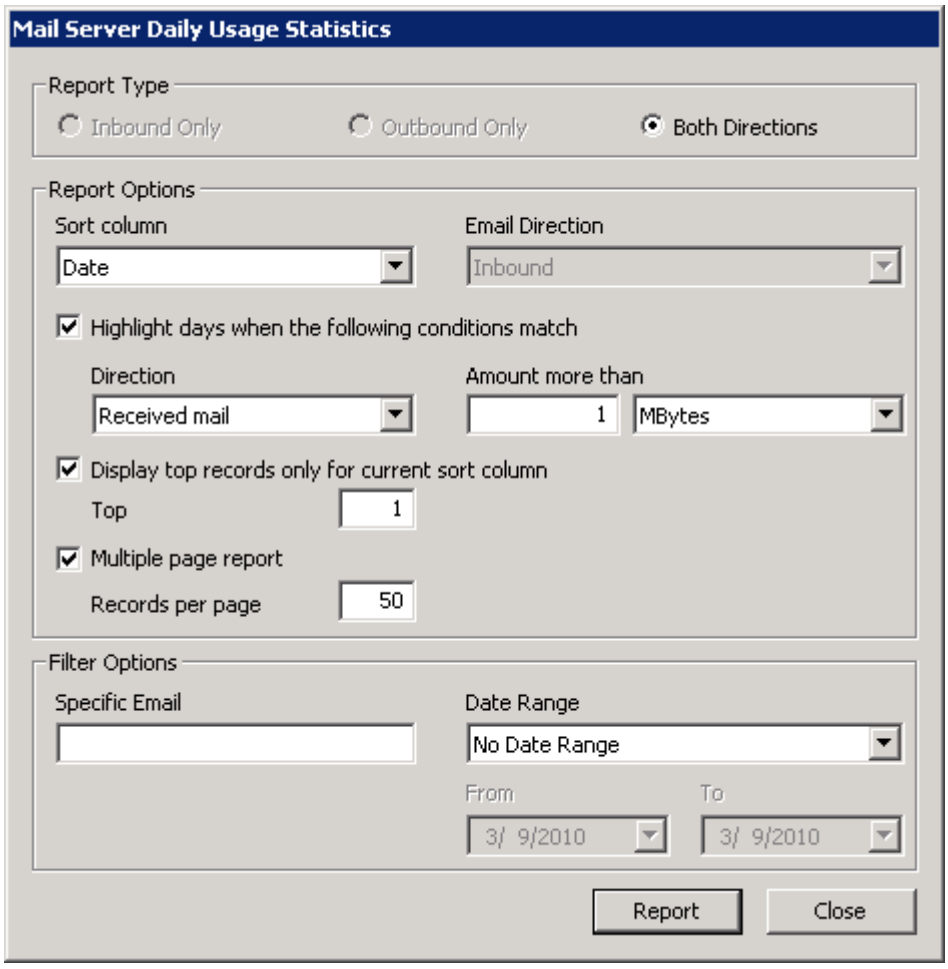
Filter options

- **Specific domain:** Limit the report to a specific domain.
- **Date Range:** Limit the report to a specific date range.

When all report options are selected, click **Report** button to generate.

3.3.7 Mail Server Daily Usage Statistics

This report gives an overview of how many emails, per day, are sent or received on the mail server where GFI MailEssentials is installed.



Screenshot 10 - Mail server daily usage statistics filter dialog

Report Type

- **Report Type:** The data for Mail Server Daily usage statistics is always reported for both inbound and outbound emails.

Report Options

- **Sort by:** Specify if report is sorted by date (since the report is per day), by number of emails, or by the total size of the emails.
- **Highlight days:** Identify the days on which you sent or received more than a number of emails or a number of megabytes of email.
- **List top:** List only the top specified number of days in the report.
- **Multi Page report:** Specify the number of days to display per page.

Filter options

- **Specific Email:** Limit the report to a specific domain.
- **Date Range:** Limit the report to a specific date range.

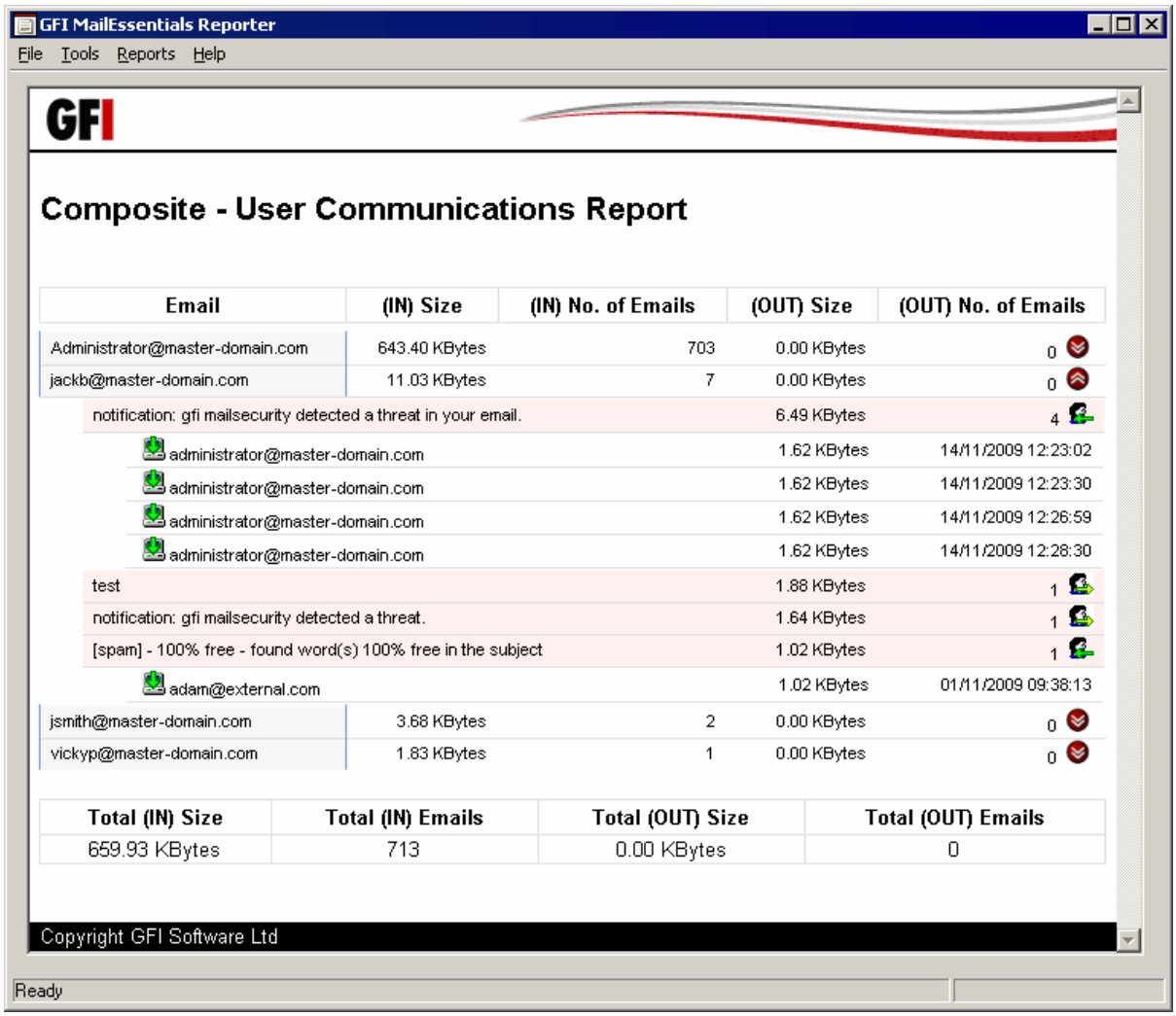
When all report options are selected, click **Report** button to generate report.

3.3.8 User Communications

The User communications report enables you to review information on what kind of emails each user has sent. Once a user communications report is generated, the user record can be expanded to list the subject of sent or received emails. Mail with the same subject is grouped. These emails can be further expanded to reveal when and to whom, email with that subject was sent.

Important notes

1. This report is a complex report that might take time to generate. It is recommended that you limit the range to a specific user or to a particular date range.


GFI MailEssentials Reporter
File Tools Reports Help
GFI
Composite - User Communications Report
Email | (IN) Size | (IN) No. of Emails | (OUT) Size | (OUT) No. of Emails
Administrator@master-domain.com | 643.40 KBytes | 703 | 0.00 KBytes | 0
jackb@master-domain.com | 11.03 KBytes | 7 | 0.00 KBytes | 0
notification: gfi mailsecurity detected a threat in your email. | 6.49 KBytes | 4
administrator@master-domain.com | 1.62 KBytes | 14/11/2009 12:23:02
administrator@master-domain.com | 1.62 KBytes | 14/11/2009 12:23:30
administrator@master-domain.com | 1.62 KBytes | 14/11/2009 12:26:59
administrator@master-domain.com | 1.62 KBytes | 14/11/2009 12:28:30
test | 1.88 KBytes | 1
notification: gfi mailsecurity detected a threat. | 1.64 KBytes | 1
[spam] - 100% free - found word(s) 100% free in the subject | 1.02 KBytes | 1
adam@external.com | 1.02 KBytes | 01/11/2009 09:38:13
jsmith@master-domain.com | 3.68 KBytes | 2 | 0.00 KBytes | 0
vickyp@master-domain.com | 1.83 KBytes | 1 | 0.00 KBytes | 0
Total (IN) Size | Total (IN) Emails | Total (OUT) Size | Total (OUT) Emails
659.93 KBytes | 713 | 0.00 KBytes | 0
Copyright GFI Software Ltd
Ready

Screenshot 11 - The user communications report shows exact email trail

Report Type

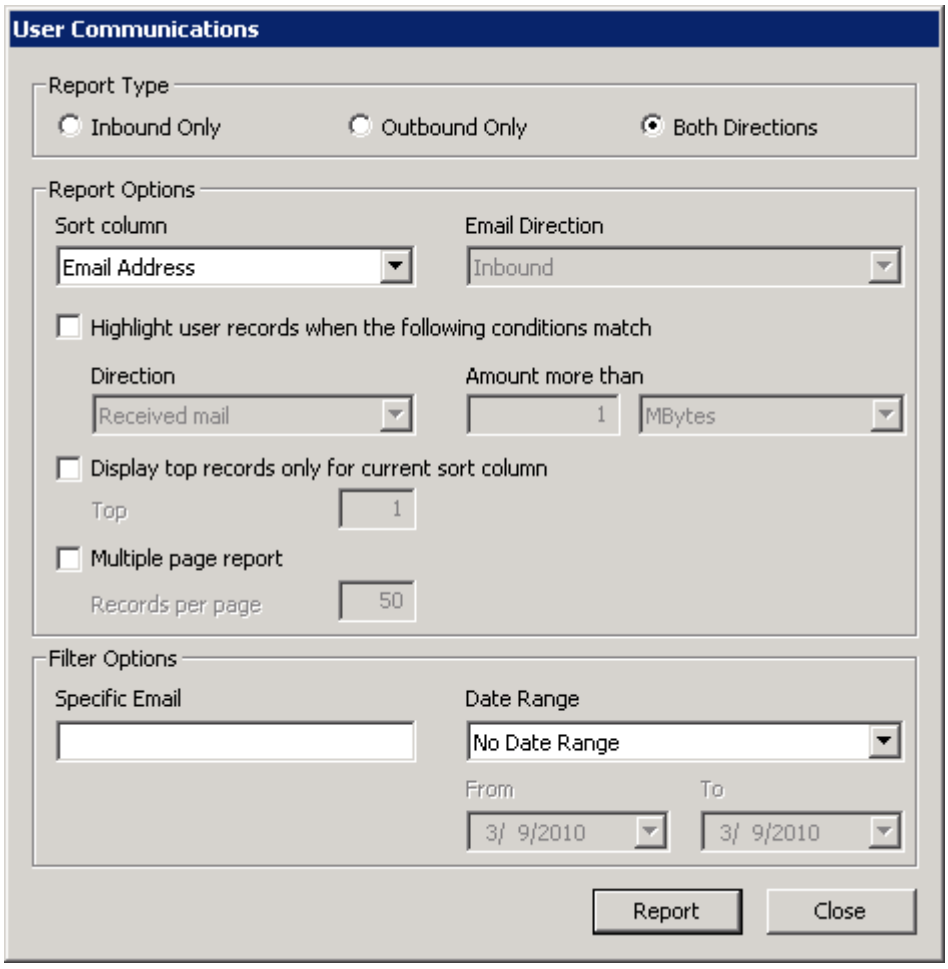
- **Report Type:** Specify reporting on inbound emails, outbound emails, or both.

Report Options

- **Sort by:** Specify if the report should be sorted by email address, by number of emails, or by the total size of the emails.
- **Highlight users:** Identify users who sent or received more than a number of emails or a number of megabytes of email.
- **List top:** List only the top specified number of users in the report.
- **Multi Page report:** Specify the number of users to display per page.

Filter options

- **Specific Email:** Limit the report to a specific email address.
- **Date Range:** Limit the report to a specific date range.



Screenshot 12 - User communications filter dialog

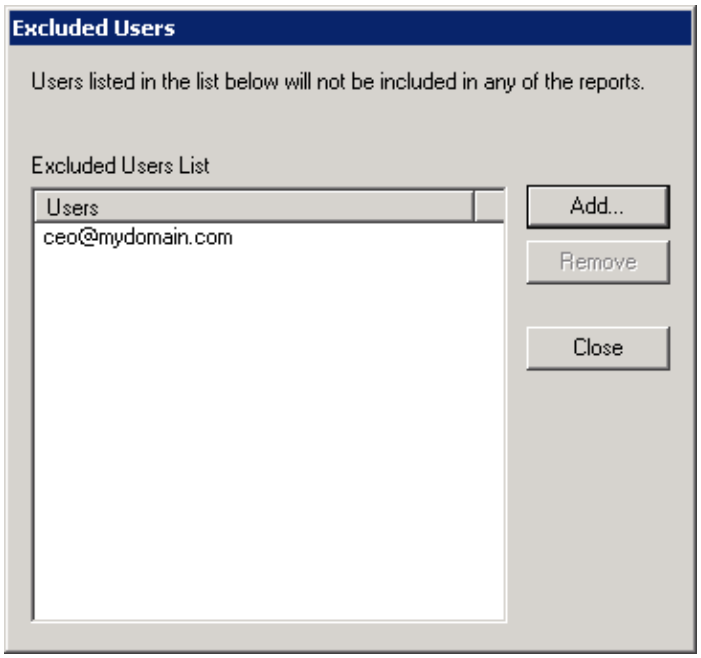
On selecting the required options, click **Report** button to generate report.

3.3.9 Miscellaneous options

» Excluding users from reports

The exclude users tool enables users to be exempted from reports

From the **Tools ► Excluded Users List** click on **Add...** button and **Add** or **Remove** SMTP email address for the user to exclude from reports.



Screenshot 13 - Excluded users dialog

» Find Tool

The find tool enables the finding of strings in reports.

From the **Tools ► Find** menu option, key in the stings to find and select **Find Next** to search for strings.

4 Routine Administration

GFI MailEssentials blocks almost all received spam emails, however as with any anti-spam solution, there can be instances where legitimate email is identified as spam (false positives) or spam emails are not identified as spam (false negatives). Given that spam makes up a high percentage of the total email flow of an organization (usually between 70% and 90% of the total mail flow), there may be thousands of emails to manage on a daily basis. A system managed solely by the administrator will be very impractical. GFI MailEssentials can be configured to allow end users determine if there were any emails that were incorrectly classified as spam or as legitimate.

4.1 Using Quarantine

The GFI MailEssentials Quarantine feature provides a central store where all inbound emails detected as spam are retained for a number of days. This ensures that users do not receive spam in their mailbox and processing on the mail server is reduced.

This chapter provides information how to use and maintain the Quarantine Store. For information how to configure Quarantine refer to **Configuring Quarantine** section in this manual.

Administrators and mail users can review quarantined emails by accessing the quarantine interface from a web browser. GFI MailEssentials can also send regular email reports to mail users to review their blocked emails.

NOTE: Only administrators have access to all quarantined spam emails. Regular mail users can only access blocked emails that were addressed to them. To configure permissions refer to **Configuring Quarantine** chapter in this manual

4.1.1 Quarantine Management

The Quarantine Management page shows statistical information and provides a quarantine search facility. Access the Quarantine Management page from:

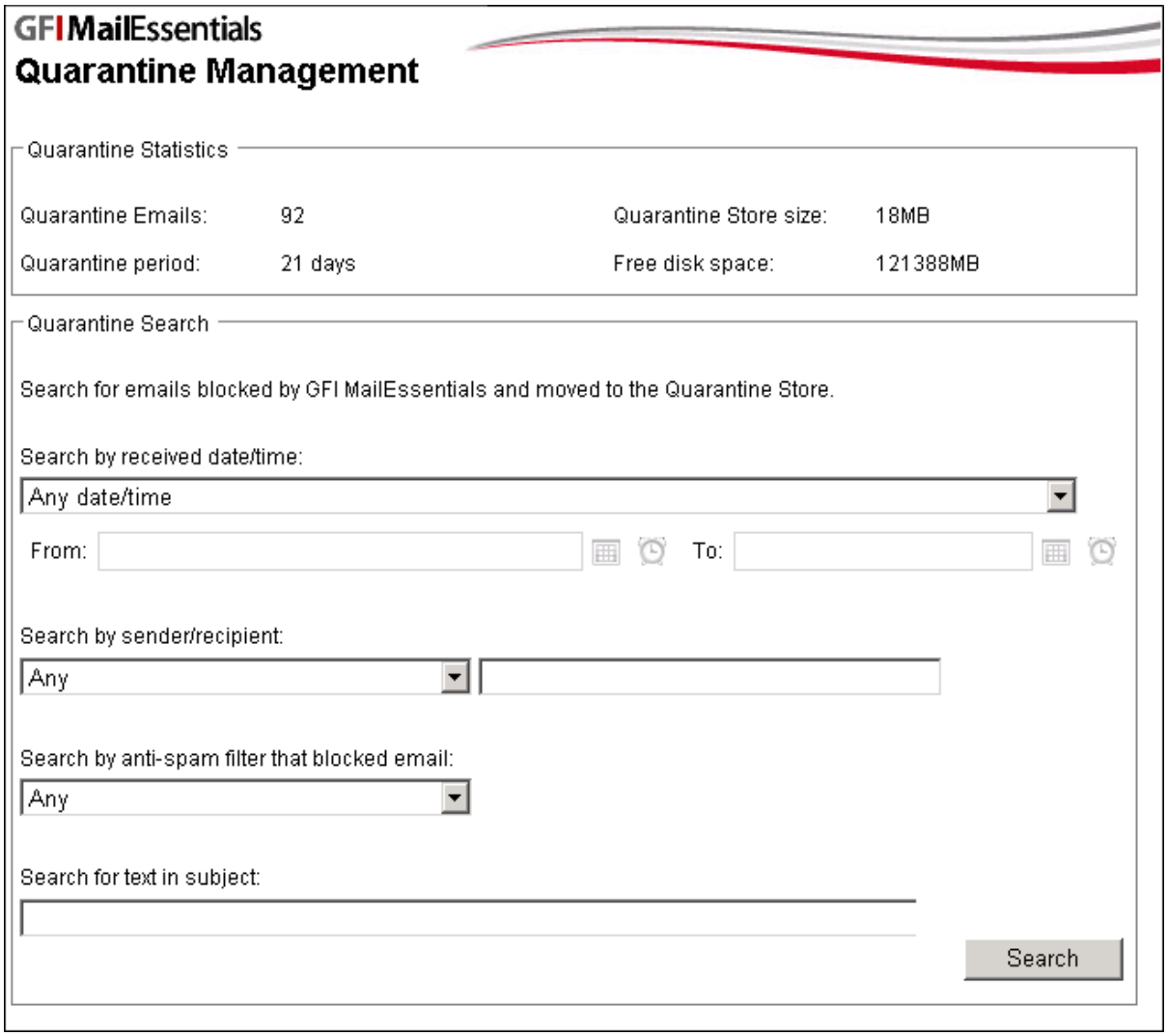
- GFI MailEssentials Configuration - navigate to Anti-Spam ► Quarantine.
- **Web interface** - Users can access the Quarantine Management page from a web browser. Key in the configured address in the following format:

  http://<*GFI MailEssentials server name*>/<*Quarantine virtual directory*>

  Example 1: http://GFIserver/SpamQuarantine

  Example 2: If the quarantine virtual directory is configured to be accessed over the web: http://www.mydomain.com/SpamQuarantine

  NOTE: If the quarantine virtual directory is secured with SSL, use https:// instead of http://.



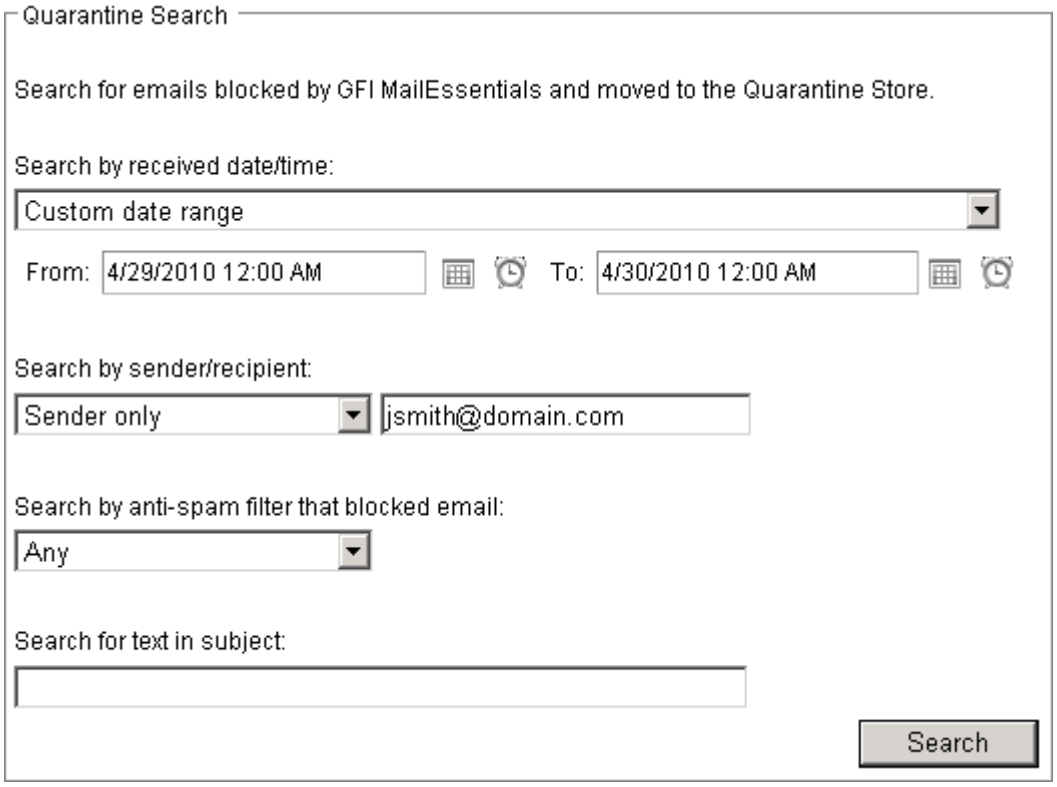
Screenshot 14 - The Quarantine Management page

The Quarantine Statistics section shows:

- **Quarantine emails** - Number of emails in Quarantine Store
- **Quarantine period** - Number of days that spam emails are retained in Quarantine Store
- **Quarantine Store size** - the quantity of disk space used by the Quarantine Store to retain spam emails and meta data.
- **Free disk space** - the amount of free disk space available on the partition where the Quarantine Store is saved. If this value is below 512MB, the Quarantine feature will stop functioning. Spam emails will be tagged and delivered to the users' mailbox until free disk space is greater than 512MB.

NOTE: To modify the Quarantine Store path or configure the number of days that spam is retained, refer to **Configuring Quarantine** section in this manual.

Searching quarantined emails



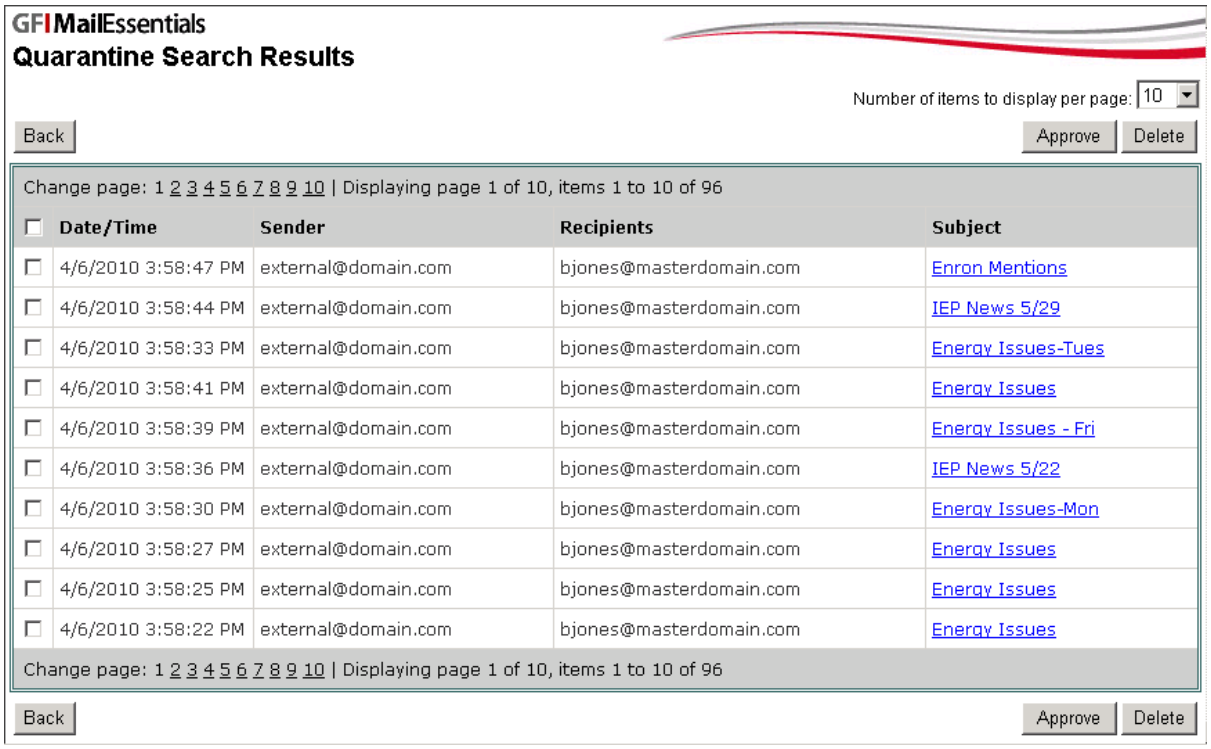
Screenshot 15 - The Quarantine search

NOTE: Only administrators can search through all quarantined spam emails. Regular mail users can only search through blocked emails that were addressed to them.

In the Quarantine Search area of the Quarantine Management page, specify any of the following search criteria:

- Date/time when email was received
- Sender or recipient
- Anti-spam filter that blocked the email
- Text in subject

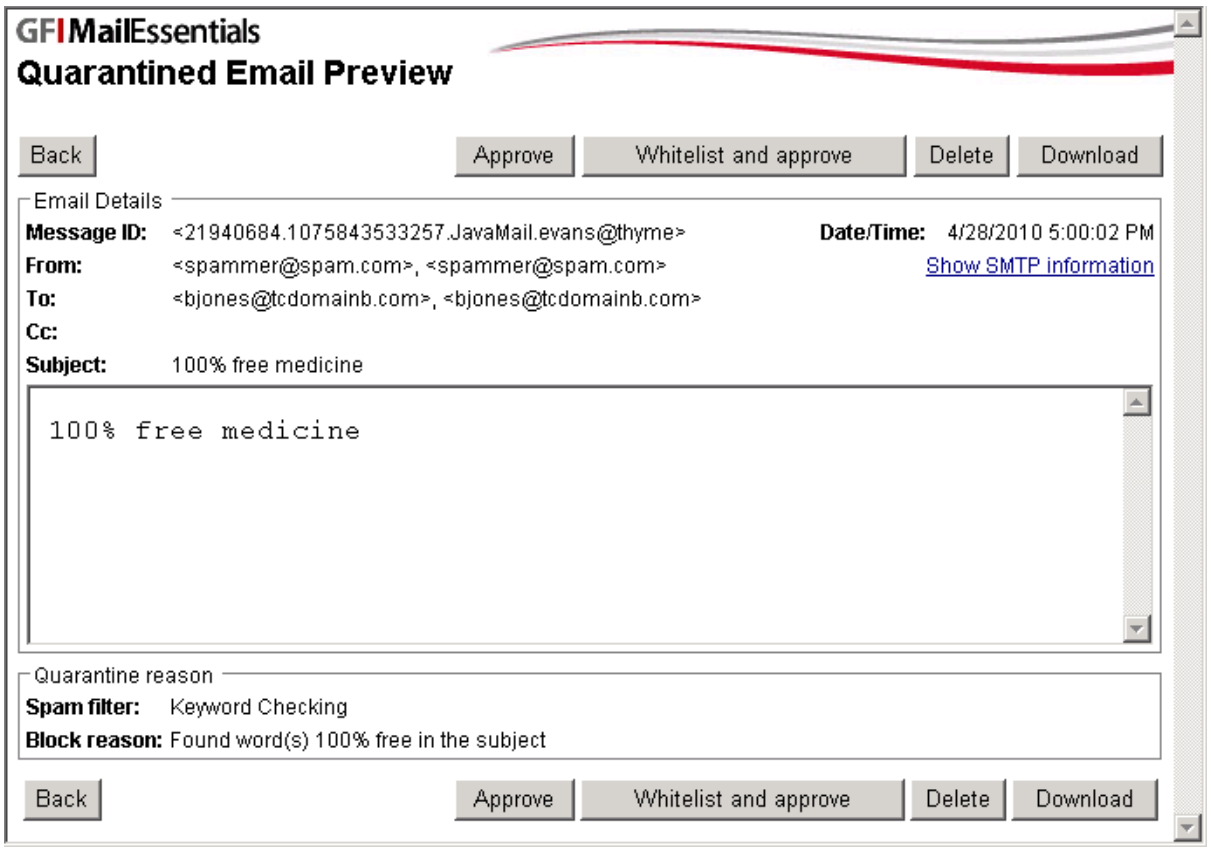
Click **Search** to display the search results.


GFI MailEssentials
Quarantine Search Results
Number of items to display per page: 10
Back
Approve
Delete
Change page: 1 2 3 4 5 6 7 8 9 10 | Displaying page 1 of 10, items 1 to 10 of 96
Date/Time
Sender
Recipients
Subject
4/6/2010 3:58:47 PM external@domain.com bjones@masterdomain.com Enron Mentions
4/6/2010 3:58:44 PM external@domain.com bjones@masterdomain.com IEP News 5/29
4/6/2010 3:58:33 PM external@domain.com bjones@masterdomain.com Energy Issues-Tues
4/6/2010 3:58:41 PM external@domain.com bjones@masterdomain.com Energy Issues
4/6/2010 3:58:39 PM external@domain.com bjones@masterdomain.com Energy Issues - Fri
4/6/2010 3:58:36 PM external@domain.com bjones@masterdomain.com IEP News 5/22
4/6/2010 3:58:30 PM external@domain.com bjones@masterdomain.com Energy Issues-Mon
4/6/2010 3:58:27 PM external@domain.com bjones@masterdomain.com Energy Issues
4/6/2010 3:58:25 PM external@domain.com bjones@masterdomain.com Energy Issues
4/6/2010 3:58:22 PM external@domain.com bjones@masterdomain.com Energy Issues
Change page: 1 2 3 4 5 6 7 8 9 10 | Displaying page 1 of 10, items 1 to 10 of 96
Back
Approve
Delete

Screenshot 16 -Quarantine search results

Select any emails that are not spam and click **Approve**.

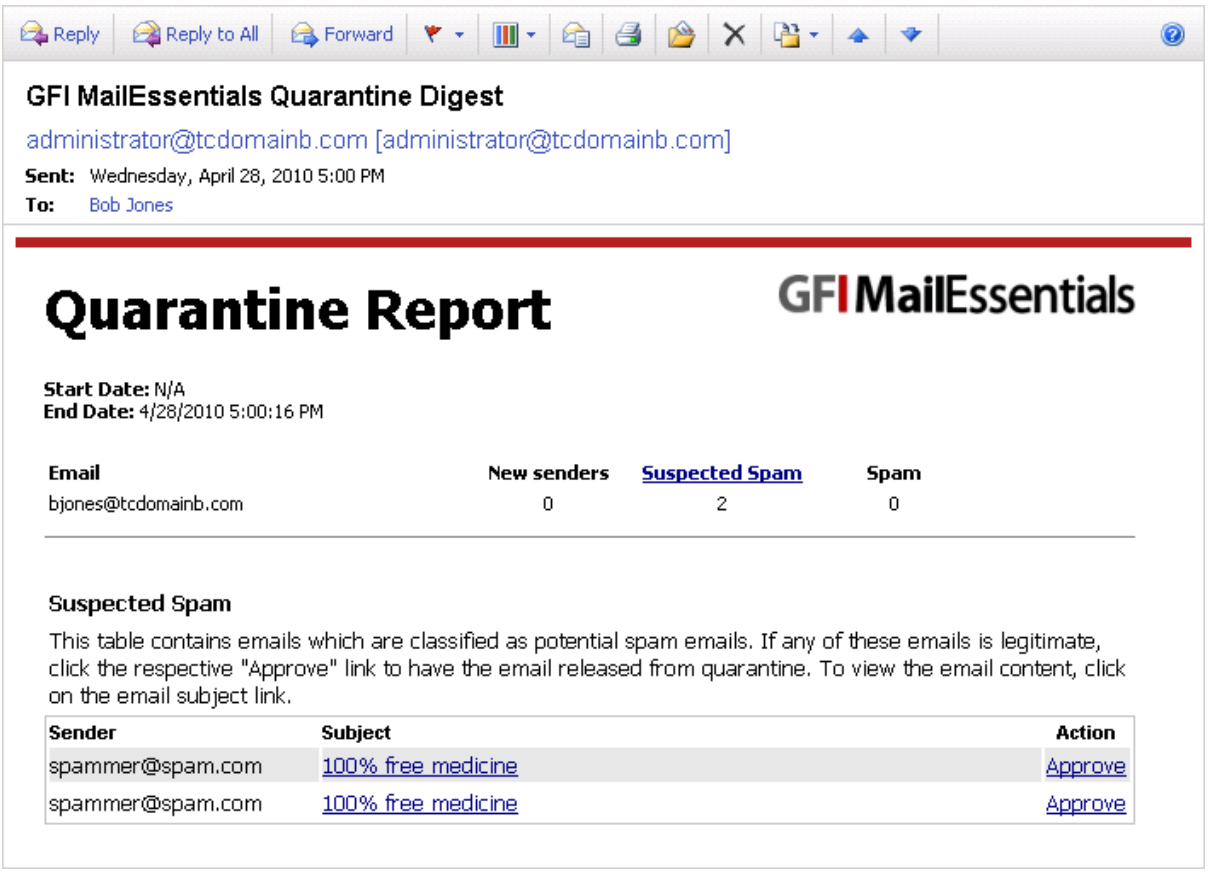
Administrators can also whitelist the sender of an email that was incorrectly identified as spam. To do this, click the email subject to preview the email and click **Whitelist and approve**.



Screenshot 17 - Previewing a quarantined email

4.1.2 User quarantine reports

You can configure GFI MailEssentials to send periodical quarantine reports to email users. This email will contain a list of emails blocked by GFI MailEssentials since the last quarantine report.



Screenshot 18 - Quarantine email report

The recipient can review the blocked emails and approve any emails that were incorrectly identified as spam. To do this, select any emails that are not spam and click **Approve**.

You can also click the email subject to preview email in web browser.

NOTE: If the email client is configured to view emails in plain text format only, emails cannot be reviewed directly from the quarantine email report. The report will notify the user that emails were blocked by GFI MailEssentials and provides a link to launch the Quarantine interface in a web browser. The user can then review and approve spam directly from the web browser.

4.2 Using Public folder scanning

4.2.1 Reviewing spam email

1. When spam emails are delivered to the user's mailbox (in Inbox, Junk E-mail folder or a custom folder) instruct the individual email users to periodically review spam emails.

2. When legitimate emails are incorrectly identified as spam (false positives), refer to the **Managing legitimate email** section below.

3. When spam emails are not detected (false negatives), refer to the **Managing spam** section below.

4.2.2 Managing legitimate email

As with any anti-spam solution, GFI MailEssentials might require some time until the optimal anti-spam filtering conditions are achieved. In cases where this is not yet achieved, there might be instances where legitimate email might be identified as spam.

In such cases users should add emails incorrectly identified as spam to the **Add to whitelist** and to the **This is legitimate email** folders to 'teach' GFI MailEssentials that the email in question is not spam.

Important notes

In Microsoft Outlook, dragging and dropping email moves the email to the selected folder. To

retain a copy of the email, hold down the **CTRL** key to copy the email rather than moving it.

Adding senders or newsletters to the whitelist

1. In the public folders, locate the **GFI AntiSpam Folders ► Add to whitelist** public folder.

2. Drag and drop emails or newsletters to the **Add to whitelist** public folder.

Adding discussion lists to the whitelist

Discussion lists are often sent out without including the recipient email address in the MIME TO and are therefore marked as spam. To receive these discussion lists, whitelist the email addresses of these valid list mailers.

1. In the public folders, locate the **GFI AntiSpam Folders ► I want this Discussion list** public folder.

2. Drag and drop discussion lists to the **I want this Discussion list** public folder.

Add ham to the legitimate email database

1. In the public folders, locate the **GFI AntiSpam Folders ► This is legitimate email** public folder.

2. Drag and drop emails to the **This is legitimate email** folder.

4.2.3 Managing spam

While GFI MailEssentials starts identifying spam emails right out of the box, there might be instances where spam makes it through undetected to the users mailbox. Typically this might be either due to configuration settings that have not yet been performed or to new forms of email spam to which GFI MailEssentials has not yet adapted itself. In both cases, these situations are resolved when GFI MailEssentials is configured to capture such spam.

NOTE: For information how to resolve issues related to emails not detected as spam refer to the Troubleshooting & support chapter in this manual.

In these cases users should add such emails to **Add to blocklist** and to the **This is spam email** folders to 'teach' GFI MailEssentials that the email in question is spam.

Important notes

1. In Microsoft Outlook, dragging and dropping email moves the email to the selected folder. To retain a copy of the email, hold down the **CTRL** key to copy the email rather than moving it.

2. Refer to the Public folder scanning section in this manual for more information how to automatically create the GFI AntiSpam folders.

Adding senders to the Email Blocklist

1. In the public folders, locate the **GFI AntiSpam Folders ► Add to blocklist** public folder.

2. Drag and drop emails to the **Add to blocklist** public folder.

Adding spam to the spam database

1. In the public folders, locate the **GFI AntiSpam Folders ► This is spam email** public folder.

2. Drag and drop the spam email to the **This is spam email** folder.

5 Configuring anti-spam

5.1 Anti-spam filters

GFI MailEssentials uses various scanning filters to identify spam:

FILTER	DESCRIPTION	ENABLED BY DEFAULT
SpamRazer	An anti-spam engine that determines if an email is spam by using email reputation, message fingerprinting and content analysis.	Yes
Directory Harvesting	Stops email which is randomly generated towards a server, mostly addressed to non-existent users.	No
Phishing	Blocks emails that contain links in the message bodies pointing to known phishing sites or if they contain typical phishing keywords.	Yes
Sender Policy Framework	Stops email which is received from domains not authorized in SPF records	No
Auto-Whitelist	Addresses to which an email is sent to, are automatically excluded from being blocked.	Yes
Whitelist	A custom list of safe email addresses	Yes
Email Blocklist	A custom list of blocked email users or domains.	Yes
IP DNS Blocklist	Checks if the email received is from senders that are listed on a public DNS list of known spammers.	Yes
URI DNS Blocklist	Stops emails which contain links to domains listed on public Spam URI Blocklists	Yes
Header checking	A module which detects spam by analyzing the email header.	Yes
Keyword checking	Spam messages are identified based on blocked keywords in the email subject or body	Yes
New Senders	Emails that have been received from senders to whom emails have never been sent before.	No
Bayesian analysis	An anti-spam technique where a statistical probability index based on training from users is used to identify spam.	No
Greylist	Identifies emails received from Non RFC compliant mail servers such as the ones normally used by spammers.	No

SpamRazer

SpamRazer is GFI's primary anti-spam engine and is enabled by default on installation. Frequent updates are released for SpamRazer that will further increase the response time to new trends of spam.

NOTE: SpamRazer is also the anti-spam engine that blocks NDR spam. For more information on GFI MailEssentials and NDR spam refer to:

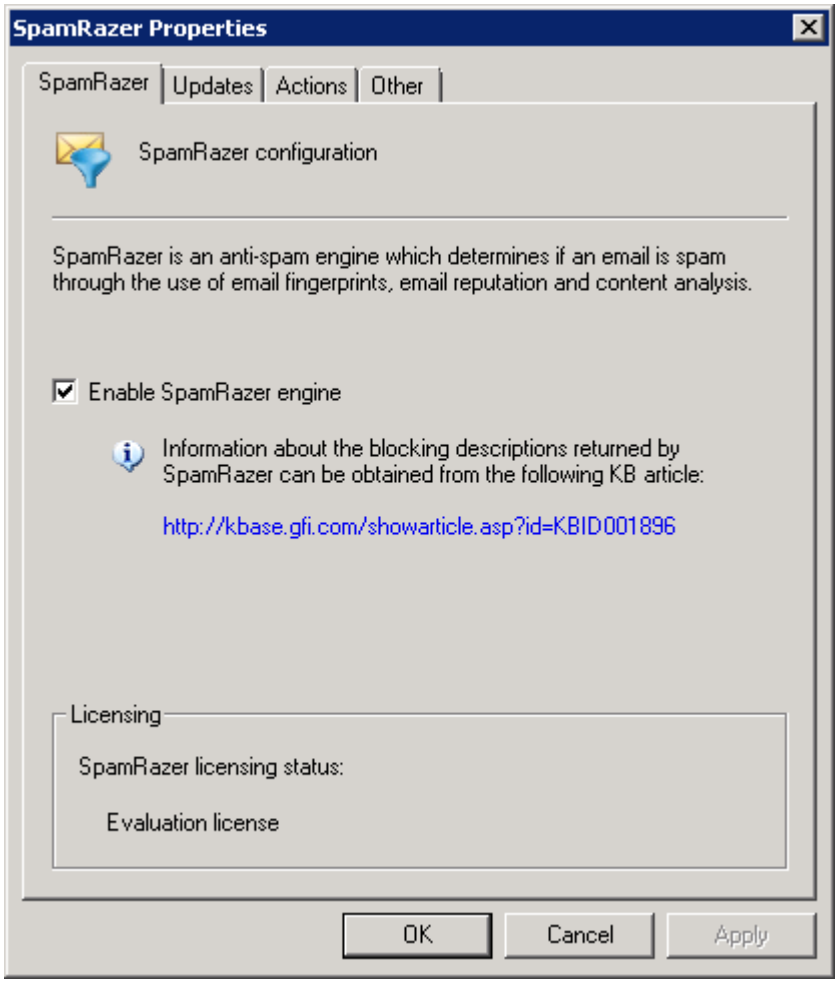
http://kbase.gfi.com/showarticle.asp?id=KBID003322

Configuring SpamRazer

NOTE 1: Disabling SpamRazer is NOT recommended.

NOTE 2: GFI MailEssentials downloads SpamRazer updates from: **http://sn92.mailshell.net**

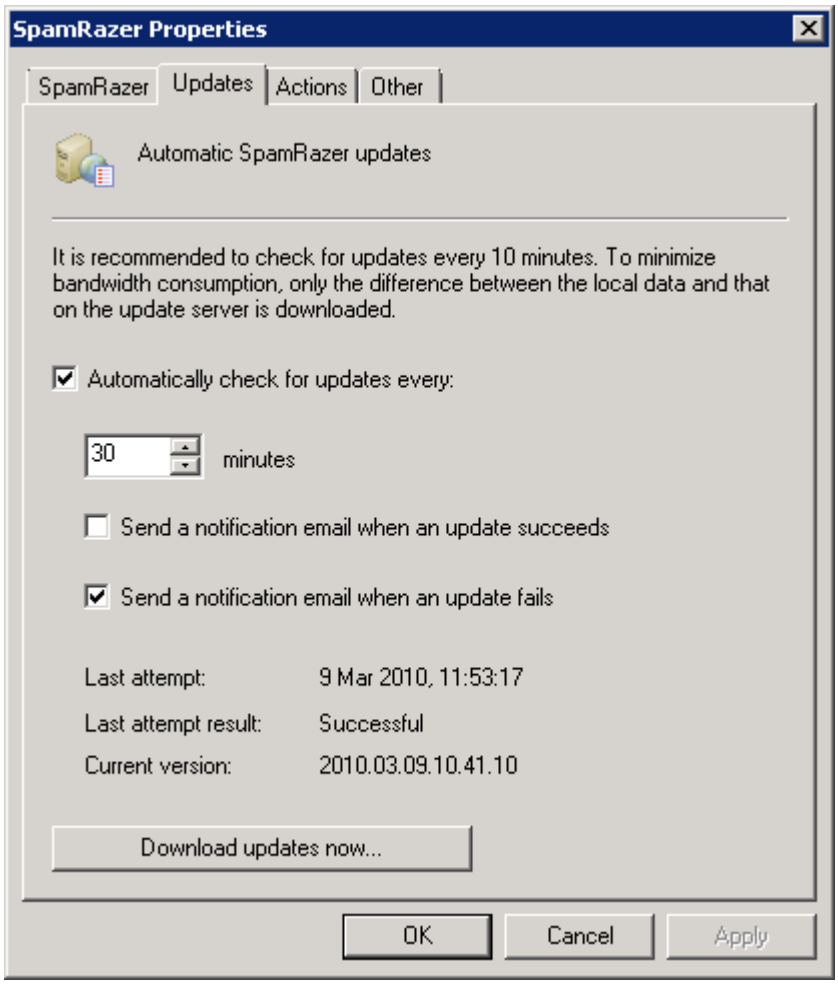
1. Select **Anti-Spam ► Anti-Spam Filters ► SpamRazer ► Properties**.



Screenshot 19 - SpamRazer Properties

2. From the **SpamRazer** tab perform any of the following actions:

» Select/unselect **Enable SpamRazer engine** checkbox to enable or disable SpamRazer.



Screenshot 20 - Automatic SpamRazer updates

3. From the **Updates** tab perform any of the following actions:

- Select/unselect **Automatically check for updates** checkbox to configure GFI MailEssentials to automatically check for and download any SpamRazer updates. Specify the time interval in minutes when to check for updates.

  NOTE: It is recommended to enable this option for SpamRazer to be more effective in detecting the latest spam trends.

- Select/unselect **Send a notification email when an update succeeds** checkbox to be informed via email when new updates are downloaded.

- Select/unselect **Send a notification email when an update fails** to be informed when a download or installation fails.

- Click **Download updates now…** to download updates.

NOTE: To download updates using a proxy server, refer to **Automatic updates** section of this manual.

4. Click **Actions** or **Other** tab to select the actions to perform on messages identified as spam. For more information refer to the **Spam Actions - What to do with spam email** section in this manual. Click **OK** to finalize your configuration.

Phishing

Phishing is an email based social engineering technique aimed at having email users disclose personal details to spammers. A phishing email is most likely crafted to resemble an official email originating from a reputable business, for example a bank. Phishing emails will usually contain instructions typically requiring users to reconfirm sensitive information such as online banking details or credit card information. Phishing emails usually include a phishing Uniform Resource Identifier (URI) that the user is supposed to follow to key in some sensitive information

on a phishing site. The site pointed to by the phishing URI might be a replica of an official site, but in reality it is controlled by whoever sent the phishing emails. When the user enters the sensitive information on the phishing site, the data is collected and used, for example, to withdraw money from bank accounts.

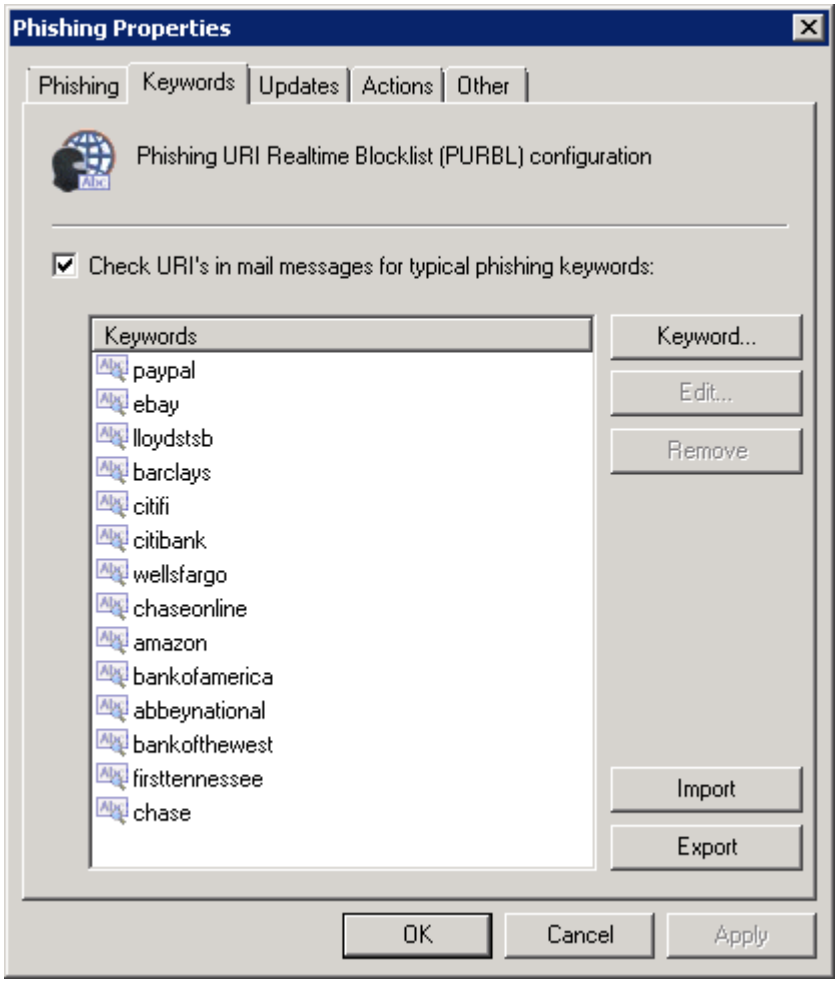
The Phishing feature detects phishing emails by comparing URIs present in the email to a database of URIs known to be used in phishing attacks. Phishing also looks for typical phishing keywords in the URIs.

The Phishing filter is enabled by default on installation.

Configuring Phishing

NOTE 1: Disabling Phishing is NOT recommended.

1. Select **Anti-Spam ► Anti-Spam Filters ► Phishing ► Properties**.



Screenshot 21 - Phishing keywords

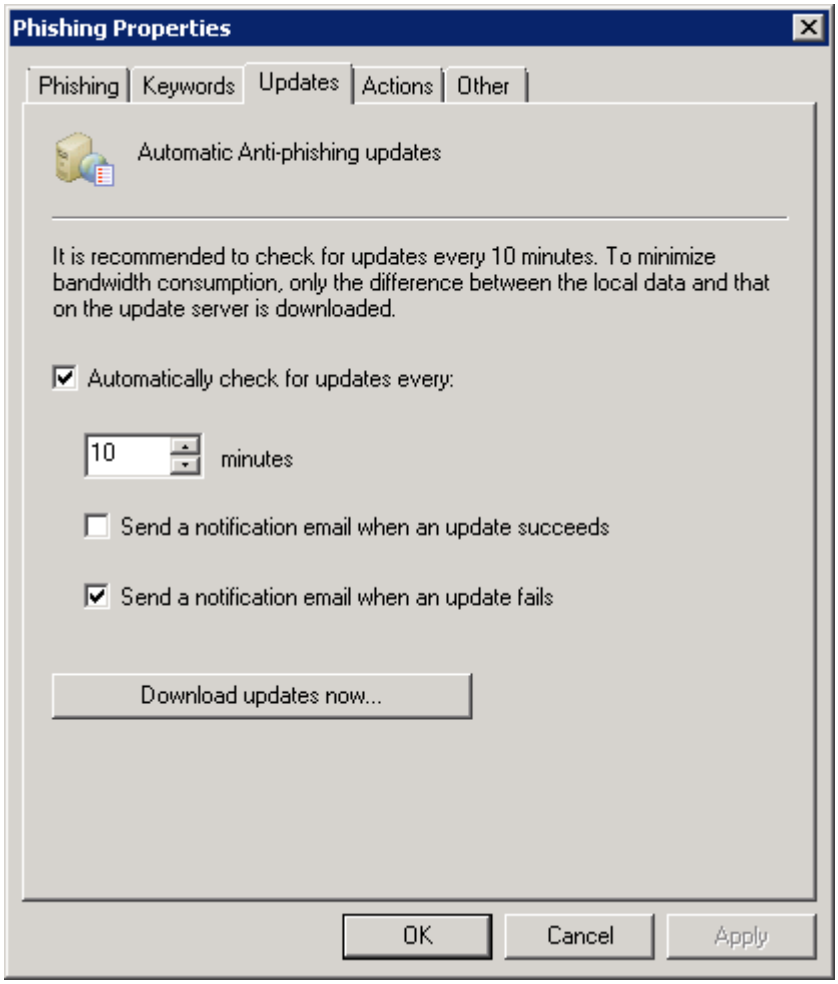
2. From the **Phishing** tab perform the following actions:

   - Select/unselect **Check mail messages for URI's to known phishing sites** option to enable/disable Phishing.

3. From the **Keywords** tab perform the following actions:

   - Select/unselect the **Check URIs in mail messages for typical phishing keywords** option to enable/disable checks for typical phishing keywords.
   - Click **Keyword** button and enter keywords in the **Enter a keyword** dialog to add keywords to the Phishing filter.
   - Select a keyword and click **Edit** or **Remove** to edit or remove a keyword previously keyed in the Phishing filter.
   - Click **Export** to export current list of keywords in XML format.

» Click **Import** button to import a keyword list previously exported to XML.


Phishing Properties
Phishing
Keywords
Updates
Actions
Other
Automatic Anti-phishing updates
It is recommended to check for updates every 10 minutes. To minimize bandwidth consumption, only the difference between the local data and that on the update server is downloaded.
Automatically check for updates every:
10
minutes
Send a notification email when an update succeeds
Send a notification email when an update fails
Download updates now...
OK
Cancel
Apply

Screenshot 22 - Automatic anti-phishing updates

4. From the **Updates** tab perform any of the following actions:

» Select/unselect **Automatically check for updates** checkbox to enable or disable the automatic check for and download of any anti-phishing updates.

NOTE: It is highly recommended to enable this option so that frequent updates enable Phishing to be more effective in detecting the latest phishing emails.

» Select/unselect **Send a notification email when an update succeeds** checkbox to be informed via email when new updates are downloaded.

» Select/unselect **Send a notification email when an update fails** to be informed when a download or installation fails.

NOTE: To download updates using a proxy server, refer to **Automatic updates** section of this manual.

5. Click **Actions** or **Other** tab to select the actions to perform on messages identified as phishing emails. For more information refer to the **Spam Actions - What to do with spam email** section in this manual. Click **OK** to finalize your configuration.

Directory harvesting

Directory harvesting attacks occur when spammers use known email addresses as a template to create other email addresses addressed to corporate or ISP email servers. Spammers send emails to randomly generated email addresses and while some email addresses may match real users, the majority of these messages is invalid and consequently floods the victim's email server.

GFI MailEssentials stops these attacks by blocking emails addressed to users not in the

organizations' Active Directory or email server.

Directory harvesting can either be configured to execute when the full email is received or at SMTP level i.e. on receiving the sending IP, email and recipients. SMTP level filtering terminates the email's connection and therefore stops the download of the full email, economizing on bandwidth and processing. In this case the connection is terminated immediately and emails are not required to go through any other anti-spam filters.

This filter is NOT enabled by default on installing GFI MailEssentials.

Configuring Directory Harvesting

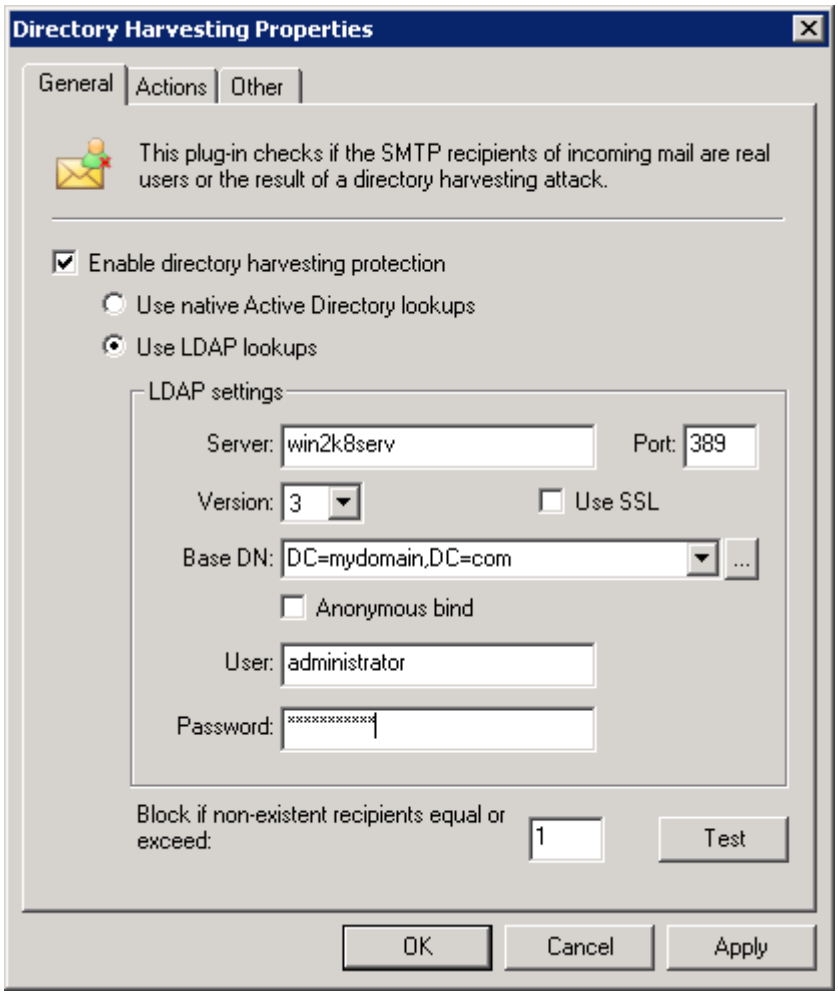
Directory Harvesting is set up in two stages:

Stage 1 - Configuring Directory Harvesting properties

Stage 2 - Selecting the Directory Harvesting method

Stage 1 - Configuring Directory Harvesting properties

1. Select **Anti-Spam ► Anti-Spam Filters ► Directory Harvesting ► Properties** and click on **Enable directory harvesting protection** option.



Screenshot 23 - The directory harvesting feature

2. Select the lookups method to use:

» **Use native Active Directory lookups** option if GFI MailEssentials is installed in Active Directory user mode.

NOTE 1: When GFI MailEssentials is installed in Active Directory user mode on a DMZ, the AD of a DMZ usually may not include all the network users (email recipients). In this case configure directory harvesting to use LDAP lookups.

NOTE 2: When GFI MailEssentials is behind a firewall, the Directory Harvesting feature might not be able to connect directly to the internal Active Directory because of Firewall

settings. Use LDAP lookups to connect to the internal Active Directory of your network and ensure to enable default port 389 on your Firewall.

» **Use LDAP lookups** to configure your LDAP settings if GFI MailEssentials is installed in SMTP mode. If your LDAP server requires authentication, unmark the **Anonymous bind** option and enter the authentication details that will be used by this feature.

NOTE 1: Specify authentication credentials using Domain\User format (for example master-domain\administrator).

NOTE 2: In an Active Directory, the LDAP server is typically the Domain Controller.

3. In the **Block if non-existent recipients equal or exceed** option specify the number of non-existent recipients that will qualify the email as spam. Emails will be blocked by Directory Harvesting if all the recipients of an email are invalid, or if the number of invalid recipients in an email exceeds the limit specified.

NOTE: Avoid false positives by configuring a reasonable amount in the **Block if non-existent recipients equal or exceed** edit box. This value should account for users who send legitimate emails with mistyped email addresses or to users no longer employed with the company. It is recommended that this value is at least '2'.

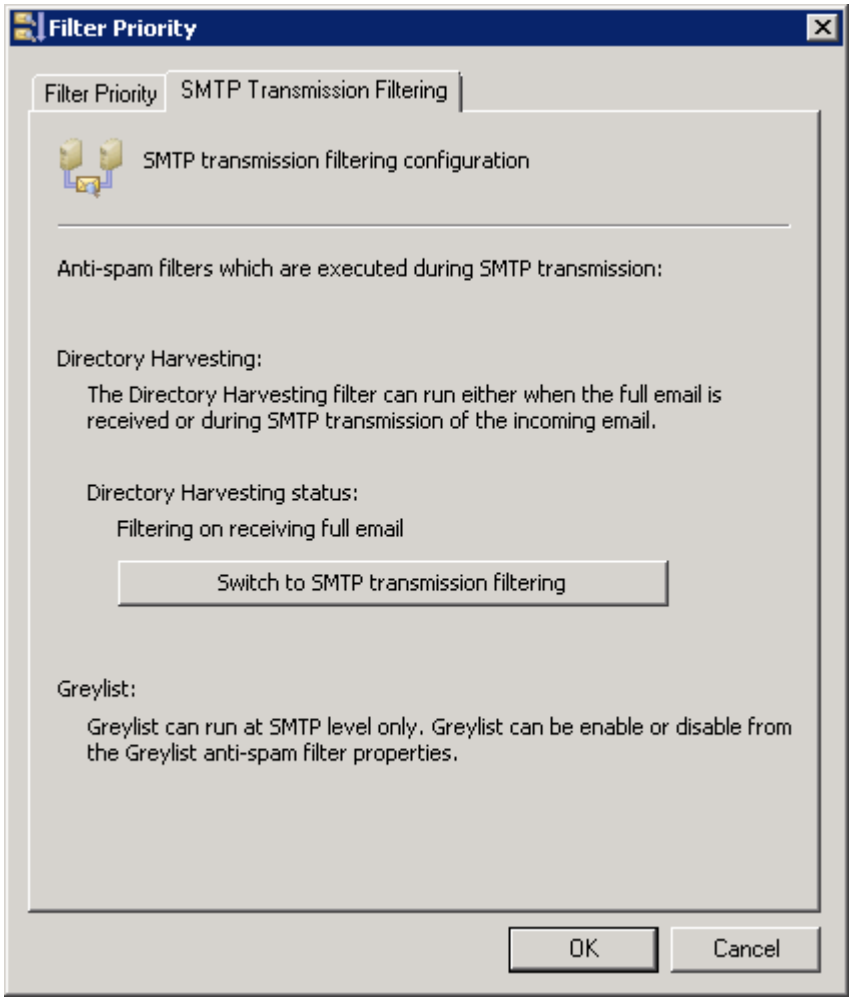
4. Click **Test** to verify Directory Harvesting settings. Specify an internal email address and click **OK** to check if Active Directory lookups can be made. Repeat the test using a non-existent email address and ensure that Active Directory lookup fails.

5. Click **Actions** or **Other** tab to select the actions to perform on messages identified as spam. For information on the actions to perform refer to the **Spam Actions - What to do with spam email** section in this manual.

NOTE: If Directory Harvesting is set to run at SMTP level, only the **Log Occurrence** option will be available in the **Actions** tab.

Stage 2 - Selecting the Directory Harvesting method

1. Navigate to **Anti-spam ► Filter Priority ► Properties**, and click the **SMTP Transmission Filtering** tab.


Filter Priority
Filter Priority
SMTP Transmission Filtering
SMTP transmission filtering configuration
Anti-spam filters which are executed during SMTP transmission:
Directory Harvesting:
The Directory Harvesting filter can run either when the full email is received or during SMTP transmission of the incoming email.
Directory Harvesting status:
Filtering on receiving full email
Switch to SMTP transmission filtering
Greylist:
Greylist can run at SMTP level only. Greylist can be enable or disable from the Greylist anti-spam filter properties.
OK
Cancel

Screenshot 24 - Anti-spam ordering dialog

2. Click the button to switch between:

- **Switch to full email filtering** - Filtering is done when the whole email is received.
- **Switch to SMTP transmission filtering** - Filtering is done during SMTP transmission by checking if the email recipients exist before the email body and attachment are received.

  NOTE: If this option is chosen, Directory Harvesting will always run before the other spam filters.

3. Click **OK** to finalize your configuration.

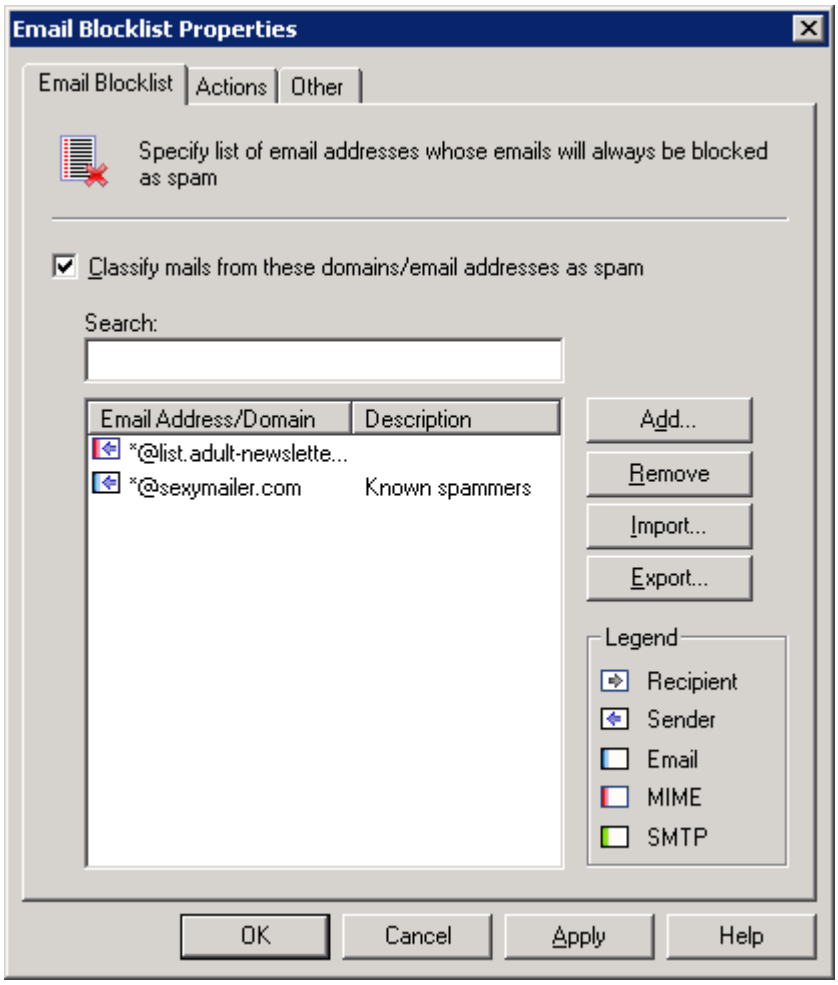
Email Blocklist

The Email Blocklist is a custom database of email addresses and domains from which you never want to receive emails.

This filter is enabled by default on installing GFI MailEssentials.

Configuring Email Blocklist

1. Select **Anti-Spam ► Anti-Spam Filters ► Email Blocklist ► Properties**.



Screenshot 25 - The email blocklist

2. From the **Email Blocklist** tab, configure the email addresses and domains to block.

OPTION	DESCRIPTION
Classify mails from these domains / email addresses as spam	Select/Unselect to enable/disable email blocklist.
Add	Add email addresses, email domains or an entire domain suffix to the blocklist. 1. Key in the email address, domain (for example, *@spammer.com); or an entire domain suffix (for example *@*.tv) to add to the blocklist. 2. Specify the email header field to match for the emails to be blocklisted. **NOTE:** For more information about the difference between SMTP and MIME refer to: http://kbase.gfi.com/showarticle.asp?id=KBID002678 3. (Optional) You can also add a description to the entry in the **Description** field.
Remove	Select a blocklist entry and click **Remove** to delete.
Import	Import a list of blocklist entries from a file in XML format. **NOTE:** A list of entries can be imported from a file in XML format in the same structure that GFI MailEssentials would export the list of entries.
Export	Export the list of blocklist entries to a file in XML format.
Search	Key in an entry to search for. Matching entries are filtered in the list of blocklist entries.

3. Select **Actions** or **Other** tab to select the actions to perform on spam. For a more information refer to the **Spam Actions - What to do with spam email** section in this manual.

4. Click **OK** to finalize your configuration.

IP DNS Blocklist

GFI MailEssentials supports a number of IP DNS Blocklists. These SMTP server databases contain lists of servers that are known to send spam emails. There are a number of third party IP DNS Blocklists available, ranging from reliable lists that have clearly outlined procedures for getting on or off the IP DNS Blocklist to less reliable lists. GFI MailEssentials checks the IP address that connected to the perimeter SMTP server against the IP DNS Blocklist.

GFI MailEssentials records all checked IP addresses in an internal database and will not perform further checks with the IP DNS Blocklist for the same IPs. The IP addresses are kept in the database for 4 days, or until the Simple Mail Transport Protocol (SMTP) service is restarted.

This filter is enabled by default on installing GFI MailEssentials.

Important notes

1. The DNS server must be properly configured for this feature to work. If this is not the case, time outs will occur and email traffic will be slowed down. For more information refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID001770

2. Querying an IP DNS Blocklist can be slow (depending on your connection), so email can be slowed down a little bit, especially if multiple IP DNS Blocklists are queried.

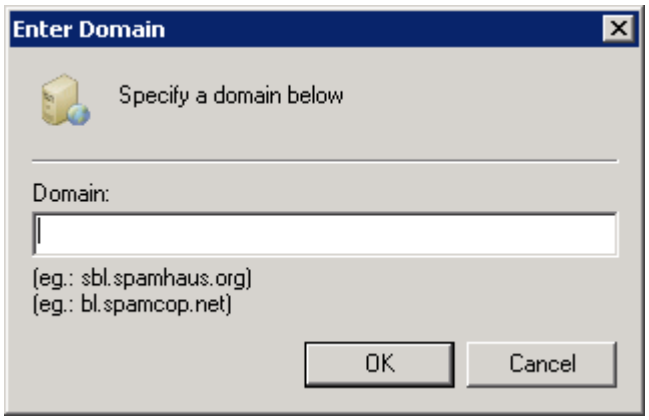
3. Ensure that all perimeter SMTP servers are specified in perimeter SMTP servers dialog to be excluded from IP DNS Blocklist filtering. For more information refer to SMTP Server settings.

Configuring IP DNS Blocklist

1. Select **Anti-Spam ► Anti-Spam Filters ► IP DNS Blocklist ► Properties**.

2. Check the **Check whether the sending mail server is on one of the following IP DNS Blocklists:** checkbox.

3. Select the appropriate IP DNS Blocklist to check incoming email against and click the **Test** button to check if the selected blocklists are available.



Screenshot 26 - Adding more IP DNS Blocklists

4. If required, add more IP DNS Blocklists to the ones already listed by clicking **Add** button and keying in the domain containing the IP DNS Blocklist.

NOTE: The order of preference for enabled IP DNS Blocklists can be changed by selecting a blocklist and clicking on the **Up** or **Down** buttons.

5. Select the **Block emails sent from dynamic IP addresses listed on SORBS.net** to enable GFI MailEssentials to detect spam sent from botnet/zombies by looking up the incoming connection IP with known Botnet/Zombie IP addresses in the Sorbs.net database.

6. Click **Apply** to save the configuration.

7. Click **Actions** or **Other** tab to select the actions to perform on messages identified as spam. For information on the actions to perform refer to the Spam Actions - What to do with spam email section in this manual.

8. Click **OK** to finalize your configuration.

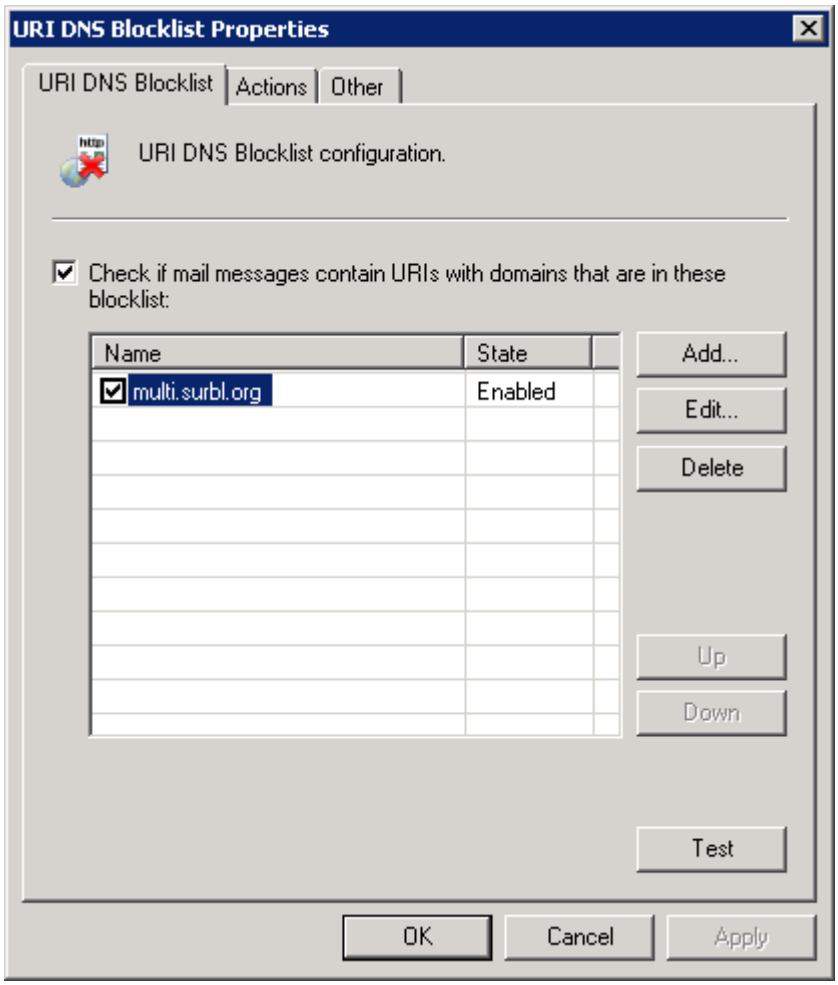
URI DNS Blocklist

A Universal Resource Identifier (URI) is a standard means of addressing resources on the Web. Common URIs such as Uniform Resource Locators (URLs) and Uniform Resource Names (URNs) are used to identify the destination of hyperlinks as well as the sources of images, information and other objects in a Web Page. URLs are most generally used in websites but can also be included as part of an email message body.

URI DNS Blocklists differ from most other Realtime Blocklists in that they are used to detect spam based on URIs found in the message body. Unlike most other RBLs, URI DNS Blocklists are not used to block spam senders. Instead, they enable blocking of messages that have spam hosts (for example web servers, domains, websites) which are mentioned in message bodies.

This filter is enabled by default on installing GFI MailEssentials.

Configuring URI DNS Blocklist



Screenshot 27 - URI DNS Blocklist properties

1. Select **Anti-Spam ► Anti-Spam Filters ► URI DNS Blocklist ► Properties**.

2. From the URI DNS Blocklist tab:

   - Check/Uncheck the Check if mail message contains URIs with domains that are in these blocklists: option to enable/disable this feature.
   - From the available list select the blocklists used as reference when checking messages using the URI DNS Blocklist feature.
   - Click **Add** button to add more URI DNS Blocklists.

3. Test the connection by clicking **Test** button and click **Apply** to save settings.

NOTE 1: Specify the full name of the domain (for example URIBL.com) containing the blocklist.

NOTE 2: Disable all other URI DNS Blocklists when enabling multi.surbl.org as this might increase

email processing time.

4. Click **Actions** or **Other** tab to select the actions to perform on messages identified as spam. For information on the actions to perform refer to the **Spam Actions - What to do with spam email** section in this manual.

5. Click **OK** to finalize your configuration.

Sender Policy Framework (SPF)

The Sender Policy Framework filter is based on a community-based effort, which requires that the senders publish their mail server in an SPF record. This filter detects forged senders.

» **Example:** If an email is sent from xyz@CompanyABC.com then companyABC.com must publish an SPF record in order for SPF to be able to determine if the email was really sent from the companyABC.com network or whether it was forged. If an SPF record is not published by CompanyABC.com, the SPF result will be 'unknown'.

For more information on SPF and how it works, visit the Sender Policy Framework website at: **http://www.openspf.org**.

The SPF filter is NOT enabled by default and should only be enabled in cases where you think that the threat of forged senders is high.

GFI MailEssentials does not make it a requirement to publish any SPF records. To publish SPF records use the SPF wizard at:

http://www.openspf.org/wizard.html.

Prerequisites

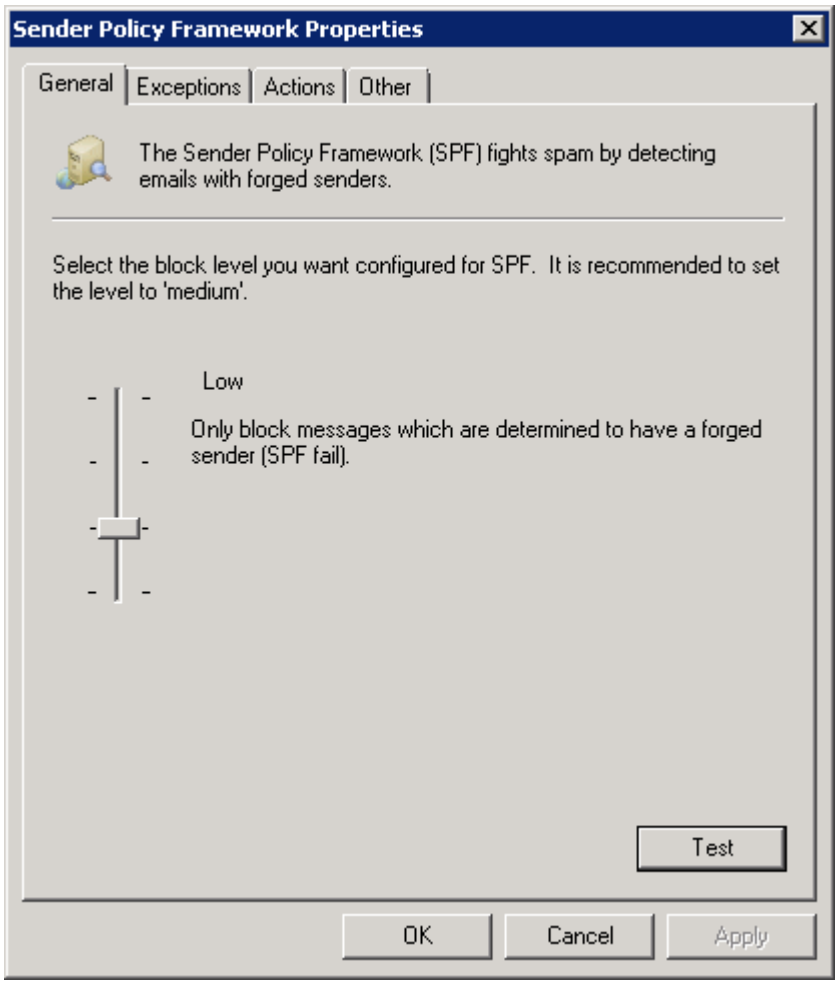
Before enabling the Sender Policy Framework filter on a non-gateway server installation:

1. Right click **Anti-spam ► Anti-Spam Settings ► Properties** and select **Perimeter SMTP Servers** tab.

2. Click **Auto Discovery** button in the Perimeter SMTP setup option to perform a DNS MX lookup and automatically define the IP address of your perimeter SMTP server.

Configuring the Sender Policy Framework

1. Select **Anti-Spam ► Anti-Spam Filters ► Sender Policy Framework ► Properties**.


Sender Policy Framework Properties
General
Exceptions
Actions
Other
The Sender Policy Framework (SPF) fights spam by detecting emails with forged senders.
Select the block level you want configured for SPF. It is recommended to set the level to 'medium'.
Low
Only block messages which are determined to have a forged sender (SPF fail).
Test
OK
Cancel
Apply

Screenshot 28 - Configuring the SPF block level

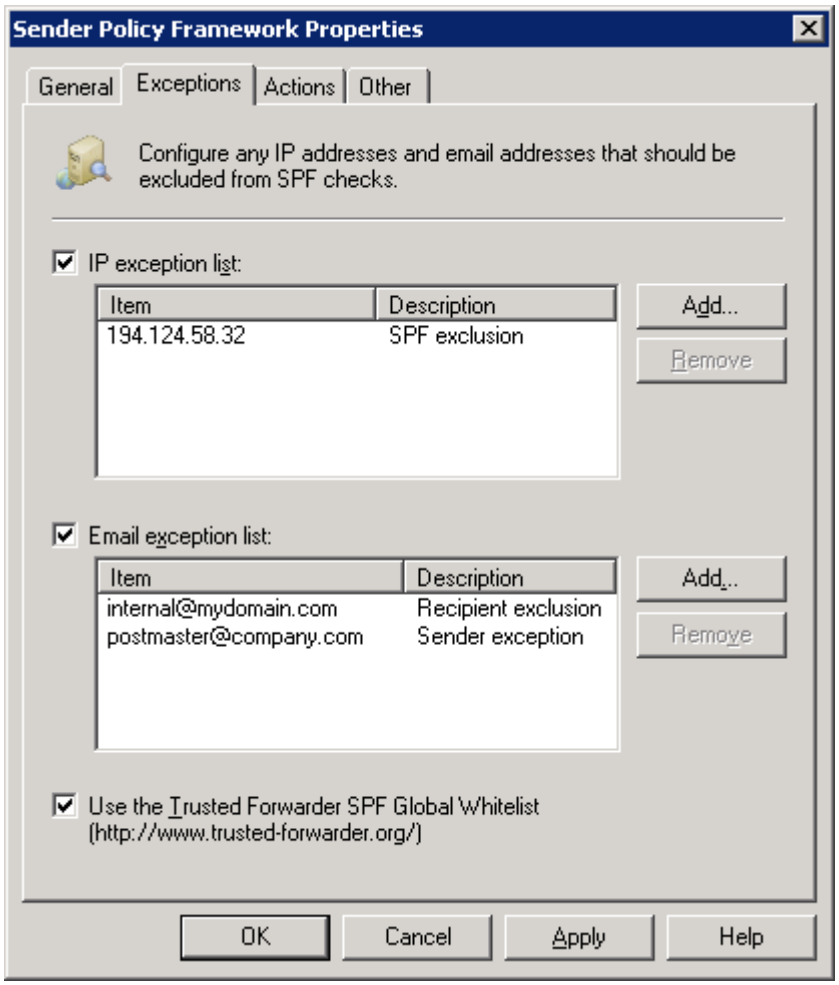
2. Define the sensitivity of the SPF test using the slider and click **Apply**. Choose between four levels:

- **Never**: Do not block any messages. SPF tests are omitted.
- **Low:** Only block messages that are determined to have a forged sender. This option treats any message with forged senders as spam.
- **Medium**: Block messages which appear to have a forged sender. This option treats all messages that appear to have a forged sender as spam.

  NOTE: This is the default and recommended setting.
- **High:** Block all messages that are not proven to be from a legitimate sender. This option treats all email as spam, unless it could be proven that the sender is not forged.

  NOTE: Since the majority of mail servers do not yet have an SPF record, this option is not recommended.

3. Test the DNS settings/services, by clicking on **Test**.



Screenshot 29 - Configuring the SPF exceptions

4. Select the **Exceptions** tab to configure IP addresses and recipients to exclude from SPF checks:

- **IP exception list:** Entries in this list automatically pass SPF checks. Select **Add** to add a new IP address or select entries from the list and click **Remove** button to remove entries. To disable the IP exception list unselect the **IP exception list** checkbox.

  NOTE: When adding IP addresses to the IP exception list, you can also add a range of IP addresses using the CIDR notation.

- **Email exception list:** This option ensures that certain email senders or recipients are excluded from SPF checking, even if the messages are rejected. An email address can be entered in any of the following three ways:
  - localpart - 'abuse' (matches 'abuse@abc.com', 'abuse@xyz.com', etc...)
  - domain - '@abc.com' (matches 'john@abc.com', 'jill@abc.com', etc...)
  - complete - 'joe@abc.com' (only matches 'joe@abc.com')

- **Trusted Forwarder SPF Global Whitelist:** This whitelist (www.trusted-forwarder.org) provides a global whitelist for SPF users. It is a way of allowing legitimate email that is sent through known, trusted email forwarders.

  NOTE: By default, this setting is enabled. It is highly recommended that this option is always enabled.

5. Click **Actions** or **Other** tab to select the actions to perform on messages identified as phishing emails. For more information refer to the **Spam Actions - What to do with spam email** section in this manual.

6. Click **OK** to finalize your configuration.

Greylist

The Greylist filter temporarily blocks incoming emails received from unknown senders and sends a retry message. This is done since an RFC compliant SMTP server will try to resend an email if a retry message is received, while spam servers normally ignore error messages. If an email is received again after a predefined period, Greylist will:

- Store the details of the sender in a database so that when the sender sends another email, the email will not be greylisted
- Receive the email and proceed with anti-spam scanning

Greylist is NOT enabled by default.

Important Notes

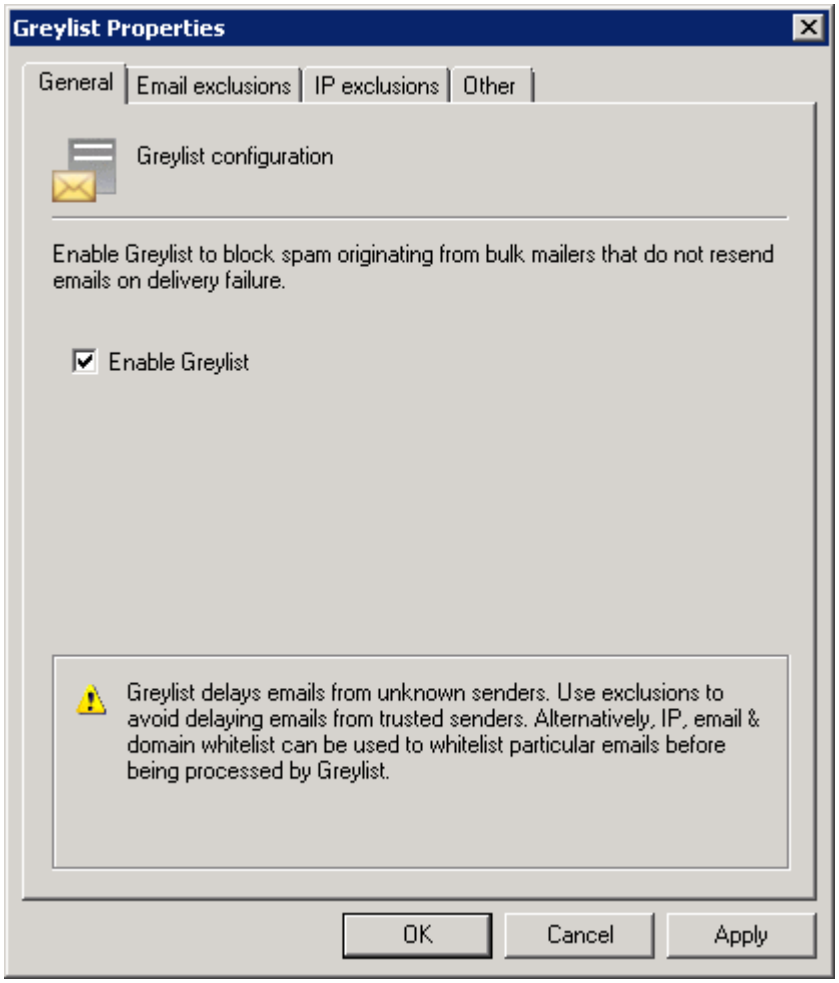
1. To enable Greylist, GFI MailEssentials must be installed on the perimeter SMTP server. For more information refer to **http://kbase.gfi.com/showarticle.asp?id=KBID003796**.

2. Greylist contains exclusion lists so that specific email addresses, domains and IP addresses are not greylisted. Exclusions must be configured when:

- Emails originating from particular email addresses, domains or IP addresses cannot be delayed
- Emails addressed to a particular local user cannot be delayed
- A legitimate sender's server does not resend a rejected email

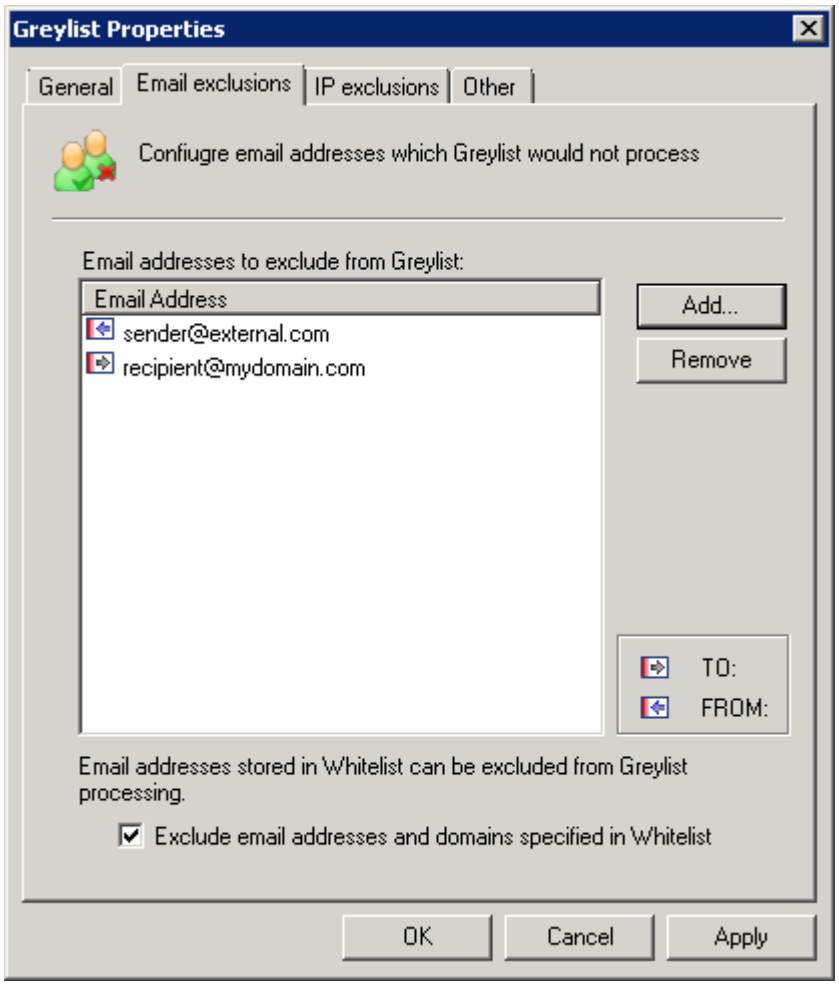
Configuring Greylist

1. Select **Anti-Spam ► Anti-Spam Filters ► Greylist ► Properties**.


Greylist Properties
General
Email exclusions
IP exclusions
Other
Greylist configuration
Enable Greylist to block spam originating from bulk mailers that do not resend emails on delivery failure.
Enable Greylist
Greylist delays emails from unknown senders. Use exclusions to avoid delaying emails from trusted senders. Alternatively, IP, email & domain whitelist can be used to whitelist particular emails before being processed by Greylist.
OK
Cancel
Apply

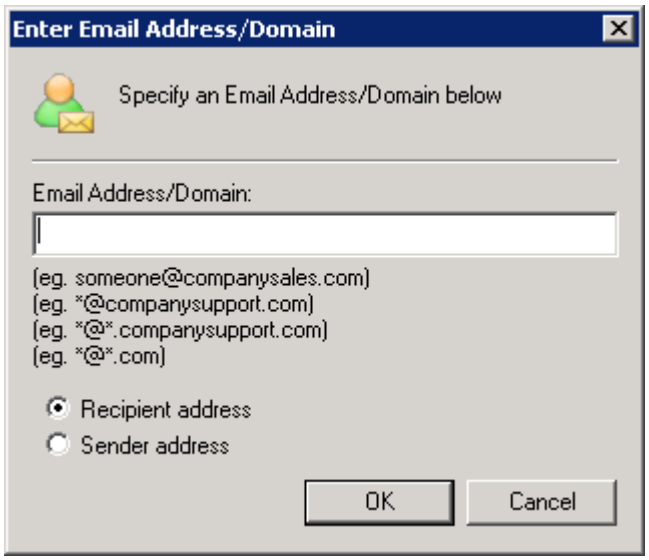
Screenshot 30 - Greylist

2. From the **General** tab select/unselect **Enable Greylist** to enable/disable Greylist.



Screenshot 31 - Email exclusions

3. Select the **Email exclusions** tab to specify any email addresses or domains that you do not want to greylist and click **Add...**.



Screenshot 32 - Adding email exclusions

4. In the **Enter Email Address/Domain** dialog specify:

- full email address; or
- emails from an entire domain (for example: *@trusteddomain.com); or
- an entire domain suffix (for example: *@*.mil or *@*.edu)

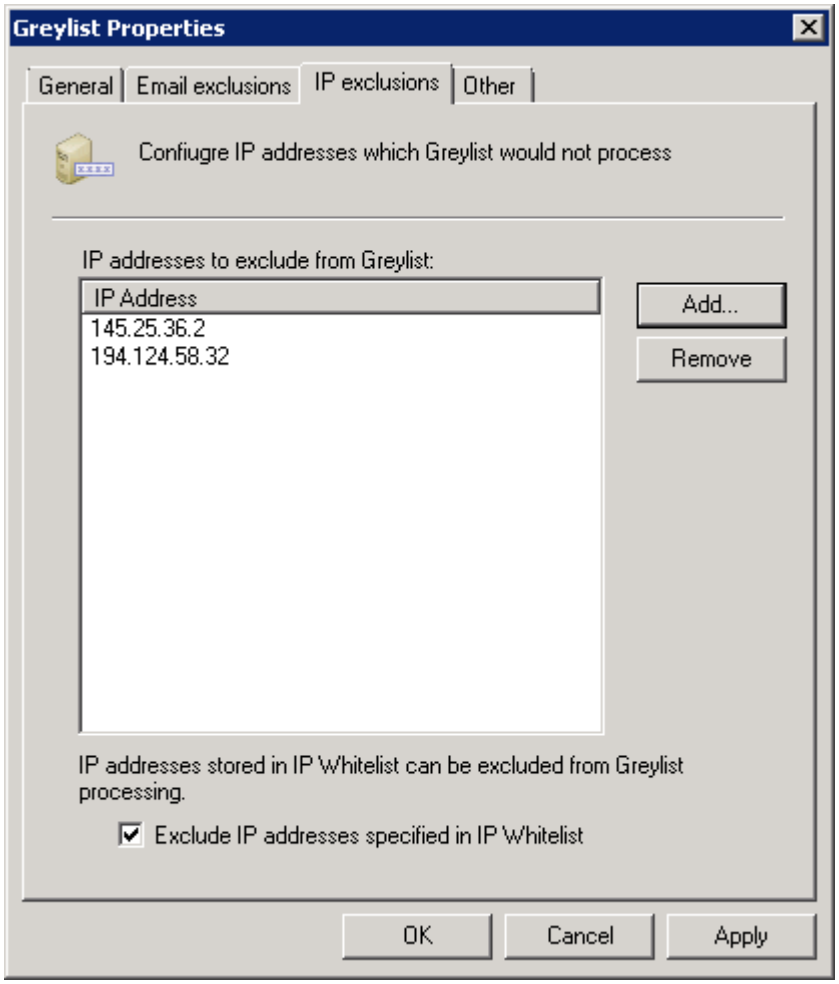
Also specify if the exclusion applies to senders or to the local recipients.

Example 1: Do not greylist emails if the recipient is administrator@mydomain.com, so that any emails sent to administrator@mydomain.com are never delayed.

Example 2: Do not greylist emails if the sender's domain is trusteddomain.com (*@trusteddomain.com), so that emails received from domain trusteddomain.com are never delayed.

Click **OK** to add the exclusion.

5. To exclude whitelisted and auto-whitelisted email addresses and domains from being greylisted and delayed, select **Exclude email addresses and domains specified in Whitelist**.



Screenshot 33 - IP address exclusions

6. Select the **IP exclusions** tab to specify any IP addresses to exclude from being greylisted. Click **Add…** and specify an IP to exclude.

7. To exclude whitelisted IP addresses from being greylisted and delayed, select **Exclude IP addresses specified in IP Whitelist**.

8. To log Greylist occurrences to a log file, navigate to the **Actions** tab and select **Log occurrence to this file**.

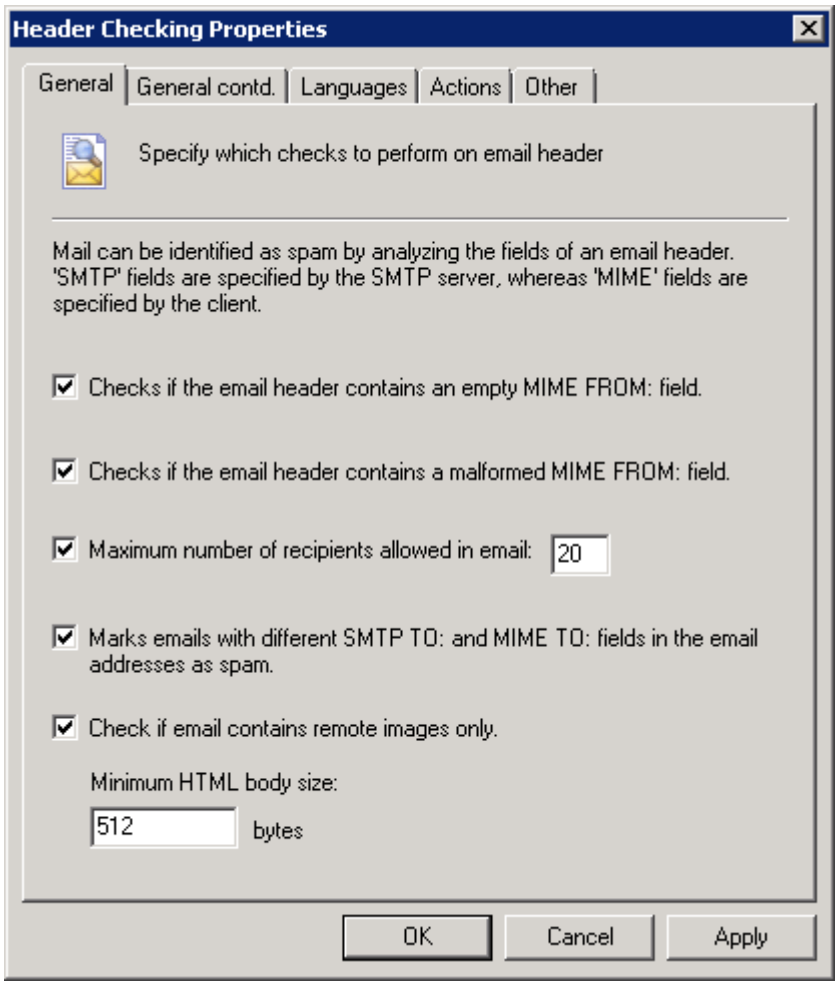
NOTE: Log files may become very large. GFI MailEssentials enables log rotation, where new log files are created periodically or when the log file reaches a specific size. To enable log file rotation navigate to **Anti-Spam ► Anti-Spam Settings**. Select **Anti-spam logging** tab, check **Enable log file rotation** and specify the rotation condition.

Header checking

The Header Checking filter analyses the email header to determine if the message is spam.

Configuring Header Checking

1. Select **Anti-Spam ► Anti-Spam Filters ► Header Checking ► Properties**.


Header Checking Properties
General
General contd.
Languages
Actions
Other
Specify which checks to perform on email header
Mail can be identified as spam by analyzing the fields of an email header. 'SMTP' fields are specified by the SMTP server, whereas 'MIME' fields are specified by the client.
Checks if the email header contains an empty MIME FROM: field.
Checks if the email header contains a malformed MIME FROM: field.
Maximum number of recipients allowed in email:
20
Marks emails with different SMTP TO: and MIME TO: fields in the email addresses as spam.
Check if email contains remote images only.
Minimum HTML body size:
512
bytes
OK
Cancel
Apply

Screenshot 34 - Header checking general tab

2. In the **General** and **General Contd.** tabs, enable, disable or configure the following parameters:

- **Checks if the email header contains an empty MIME FROM field:** Checks if the sender has identified himself in the From: field. If this field is empty, the message is marked as spam.
- **Checks if the email header contains a malformed MIME FROM: field:** Checks if the MIME from field is a correct notation as defined in the RFCs.
- **Maximum number of recipients allowed in email:** Identifies emails with large amounts of recipients and flags them as SPAM.
- **Marks email with different SMTP TO: and MIME TO: fields in the email addresses as spam:** Checks whether the SMTP to: and MIME to: fields are the same. The spammers email server always has to include an SMTP to: address. However, the MIME to: email address is often not included or is different.

  NOTE: This feature identifies a lot of spam, however some list servers do not include the MIME to: either. It is therefore recommended to whitelist newsletter sender address to use this feature.
- **Check if email contains remote images only:** Flag emails that only have remote images and a minimal amount of text as spam. Assists in identifying 'image only email' spam.
- **Verify if sender domain is valid:** Performs a DNS lookup on the domain in the MIME from field and verifies the domain validity.

  NOTE: Ensure that the DNS server is properly configured to avoid timeouts and slow email flow. Test your DNS server/services by clicking **Test** button.
- **Maximum numbers allowed in MIME FROM:** Identifies the presence of numbers in the MIME from field. Spammers often use tools that automatically create unique reply-to: addresses by using numbers in the address.

» **Checks if the email subject contains the first part of the recipient email address:** Identifies the personalized spam email, where spammers frequently include the first part of the recipient email address in the subject.

NOTE: Ensure that email addresses for which this check should not be done is configured by clicking on the **Except…** button. This enables generic email addresses to which customers reply with, for example emails from sales@company.com with a subject 'Your email to sales', not to be marked as spam

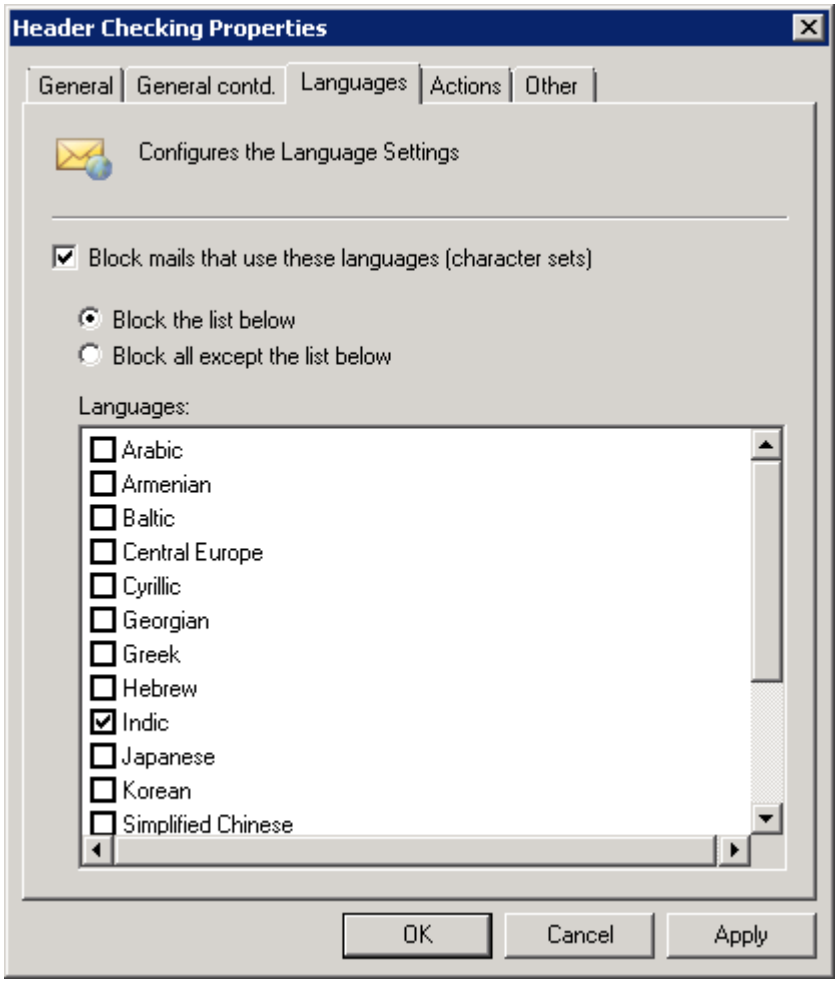
» **Check if email contains encoded IP addresses:** Checks the message header and body for URLs which have a hex/octal encoded IP (http://0072389472/hello.com) or which have a username/password combination (for example www.citibank.com@scammer.com).

- The following examples are flagged as spam:
  - *http://12312*
  - *www.microsoft.com:hello%01@123123*

» **Check if email contains embedded GIF images:** Checks if the email contains one or more embedded GIF images. Embedded GIF images are often used to circumvent spam filters.

IMPORTANT: Since some legitimate emails contain embedded GIF images, this option is prone to false positives.

» **Check if email contains attachment spam:** Checks email attachments for properties that are common to attachments sent in spam email. This helps in keeping up with the latest techniques used by spammers in using attachments to send spam.



Screenshot 35 - Language detection

3. In the Languages tab, select the **Block mails that use these languages (character sets)** option to block emails sent using character sets which are not typical of the emails received (for example Chinese or Vietnamese).

NOTE: This feature does not distinguish between languages with the same character set (for example Italian and French).

4. Click **Actions** or **Other** tab to select the actions to perform on messages identified as spam. For information on the actions to perform refer to the **Spam Actions - What to do with spam email** section in this manual.

5. Click **OK** to finalize your configuration.

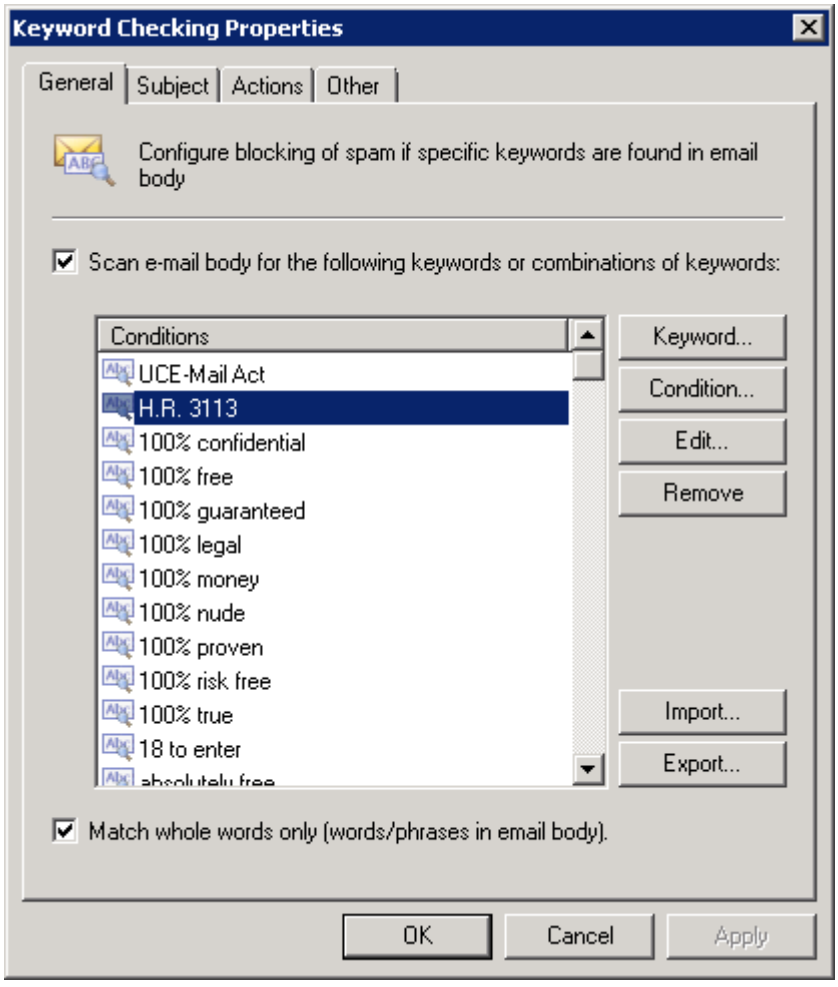
Keyword checking

Keyword checking enables the identification of spam messages based on keywords in the email being received.

This filter is NOT enabled by default.

Configuring Keyword Checking

1. Select **Anti-Spam ► Anti-Spam Filters ► Keyword Checking ► Properties**.

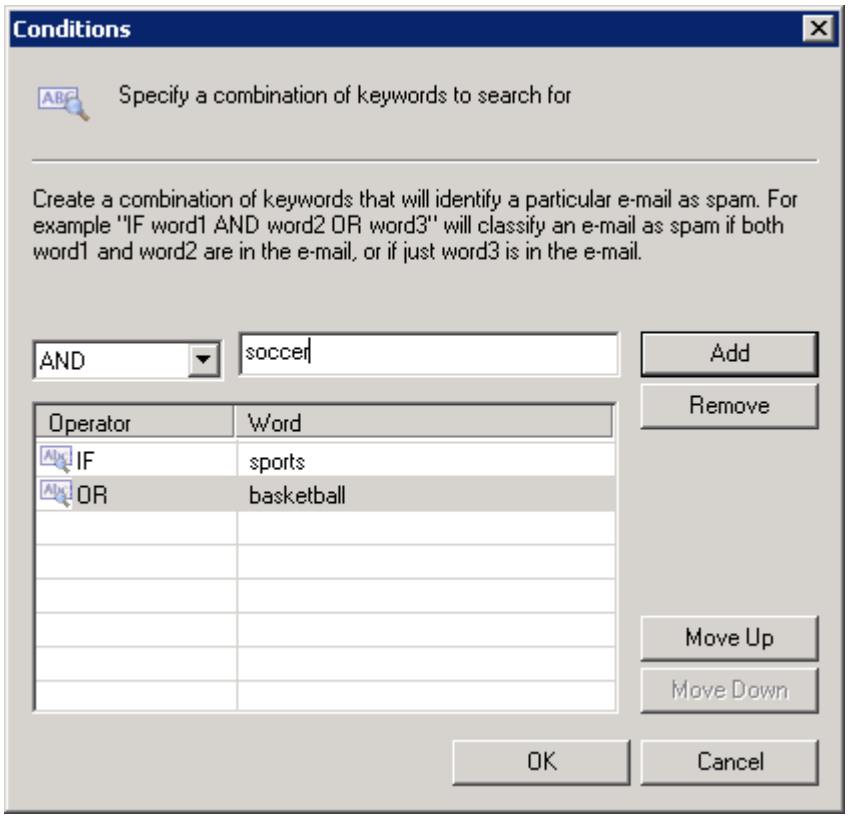


Screenshot 36 - Anti-spam keyword checking properties

2. Choose **Scan e-mail body for the following keywords or combinations of keywords:** checkbox to enable this feature.

3. Click **Keyword** button to enter keywords. If multiple words are keyed in, then GFI MailEssentials will search for that phrase.

- **Example:** For 'Basketball sports', GFI MailEssentials will check for the phrase 'Basketball sports'. Only this phrase would activate the rule, not the word basketball OR sports separated by some other words.


Conditions
Specify a combination of keywords to search for
Create a combination of keywords that will identify a particular e-mail as spam. For example "IF word1 AND word2 OR word3" will classify an e-mail as spam if both word1 and word2 are in the e-mail, or if just word3 is in the e-mail.
AND
soccer
Add
Remove
Operator
Word
IF
sports
OR
basketball
Move Up
Move Down
OK
Cancel

Screenshot 37 - Adding a condition

4. Add logical operators by clicking the **Condition…** button.

NOTE: Conditions are combinations of keywords using the operands IF, AND, AND NOT, OR, OR NOT. Using conditions specify combinations of words that must appear in the email.

- **Example:** A condition 'If Word1 AND Word2' will check for Word1 and Word2. Both words would have to be present in the email to activate the rule.

To add a condition, click the **Condition…** button.

5. Choose the **Subject** tab and check the **Scan e-mail subject for the following keywords or combinations of keywords** checkbox. Configure the words to check for in the subject of the message.

- To enter single words or phrases without logical operators, click the **Keyword…** button.
- To enter keywords combined with logical operators click the **Condition…** button.
- To edit an entry, select the entry and click **Edit…**.
- To delete an entry, select the entry and click **Remove**.

6. You can also apply the list of subject keywords to filter the senders' display name. Senders display names that contain matching keywords are marked as spam. To enable this option, select **Apply the keywords list to also scan senders' display names**.

7. Click **Actions** or **Other** tab to select the actions to perform on messages identified as spam. For information on the actions to perform refer to the **Spam Actions - What to do with spam email** section in this manual.

8. Click **OK** to finalize your configuration.

Bayesian analysis

The Bayesian filtering is an anti-spam technology in use within GFI MailEssentials that employs adaptive techniques based on artificial intelligence algorithms, hardened to withstand the widest range of spamming techniques available today.

For more information how the Bayesian filter works, how it can be configured and how it can be trained refer to **Appendix - Bayesian Filtering** in this manual.

NOTE: The Bayesian anti-spam filter is disabled by default.

IMPORTANT: Allow at least a week for the Bayesian filter to achieve its maximum performance after enabling it. This is required because the Bayesian filter acquires its highest detection rate when it adapts to your email patterns.

Configuring the Bayesian filter

Configuring the Bayesian filter requires 2 stages:

Stage 1: Training the Bayesian filter

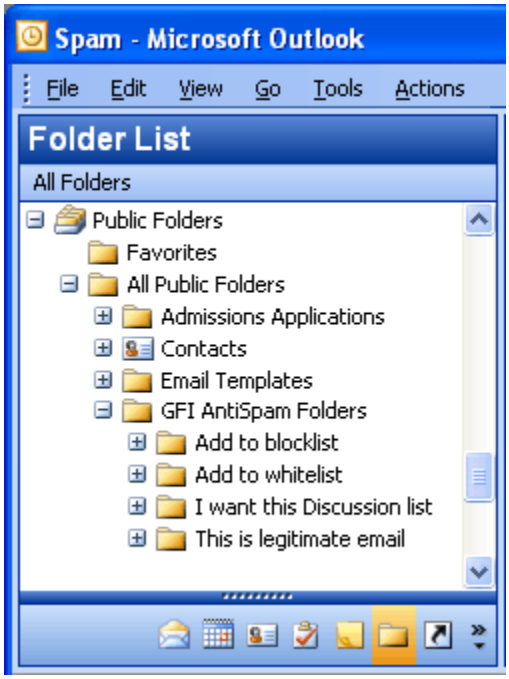
Stage 2: Enabling the Bayesian filter

Stage 1: Training the Bayesian filter

The Bayesian filter can be trained in two ways:

1. Automatically, through outbound emails.

GFI MailEssentials collects legitimate email (ham) by scanning outbound email. The Bayesian filter can be enabled after it has collected at least 500 outbound emails (If you send out mainly English email) or 1000 outbound mails (If you send out non-English email).



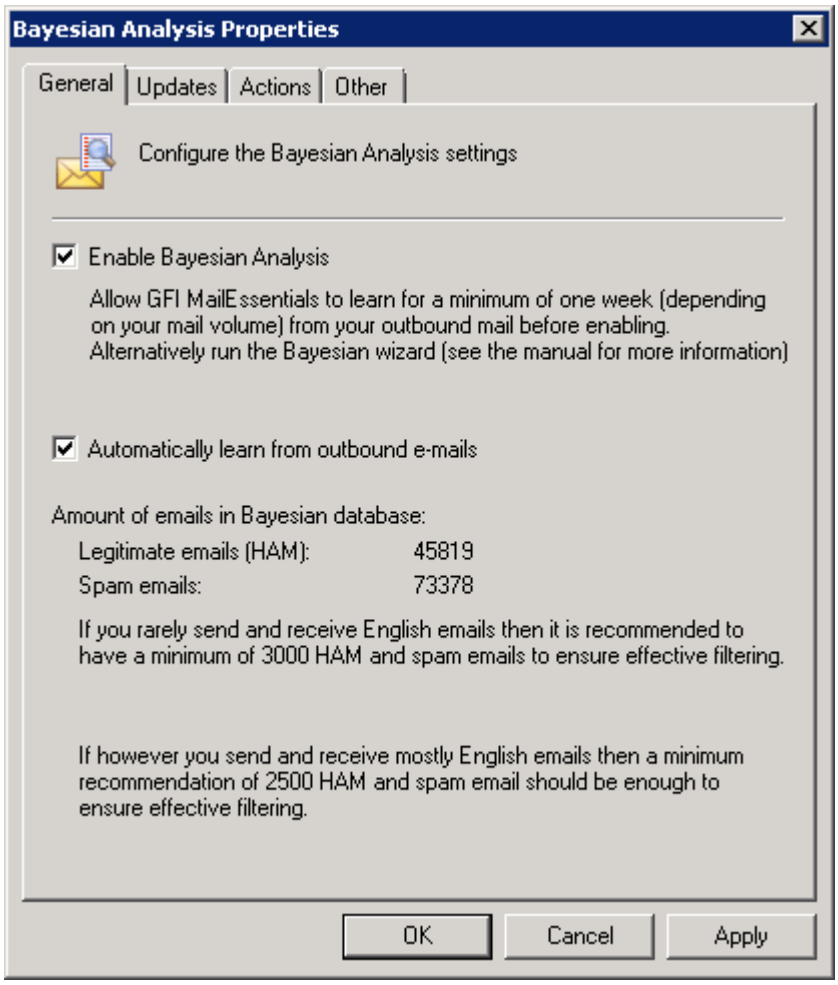
Screenshot 38 - Supplying ham to the Bayesian filter

2. Manually, through existing email.

Copying between 500-1000 mails from your sent items to the **This is legitimate email** sub folder in the **GFI AntiSpam Folders** public folders trains the Bayesian filter in the same way as live outbound email sending.

Stage 2: Enabling the Bayesian filter

After the Bayesian filter is trained, it must be enabled.


Bayesian Analysis Properties
General
Updates
Actions
Other
Configure the Bayesian Analysis settings
Enable Bayesian Analysis
Allow GFI MailEssentials to learn for a minimum of one week (depending on your mail volume) from your outbound mail before enabling.
Alternatively run the Bayesian wizard (see the manual for more information)
Automatically learn from outbound e-mails
Amount of emails in Bayesian database:
Legitimate emails (HAM): 45819
Spam emails: 73378
If you rarely send and receive English emails then it is recommended to have a minimum of 3000 HAM and spam emails to ensure effective filtering.
If however you send and receive mostly English emails then a minimum recommendation of 2500 HAM and spam email should be enough to ensure effective filtering.
OK
Cancel
Apply

Screenshot 39 - Bayesian analysis properties

1. From the GFI MailEssentials configuration console, select **Anti-Spam** ► **Anti-Spam Filters** ► **Bayesian Analysis** ► **Properties**. From the **General** tab select **Enable Bayesian Analysis** checkbox.

2. Ensure that **Automatically learn from outbound emails** option is enabled. This continuously updates the legitimate email database with data from outbound emails.

3. In the **Updates** tab, configure the frequency of updates to the spam database by enabling **Automatically check for updates** and configuring an hourly interval.

NOTE 1: Click the **Download updates now** button to immediately download any updates.

NOTE 2: For more information how to select preferred servers, and how to download updates using a proxy server, refer to **Automatic updates** of this manual.

4. Click **Actions** or **Other** tab to select the actions to perform on messages identified as spam. For information on the actions to perform refer to the **Spam Actions - What to do with spam email** section in this manual.

5. Click **OK** to finalize your configuration.

Whitelist

The Whitelist contains lists of criteria that identify legitimate email. Emails that match these criteria are not scanned by anti-spam filters and are always delivered to the recipient. Emails can be whitelisted using the following criteria:

- Sender's email address, email domain or IP address
- Senders to whom an email was previously sent (Auto-whitelist)
- Recipient (exclude local email addresses from having emails filtered)
- Keywords in email body or subject

The whitelist and autowhitelist features are enabled by default.

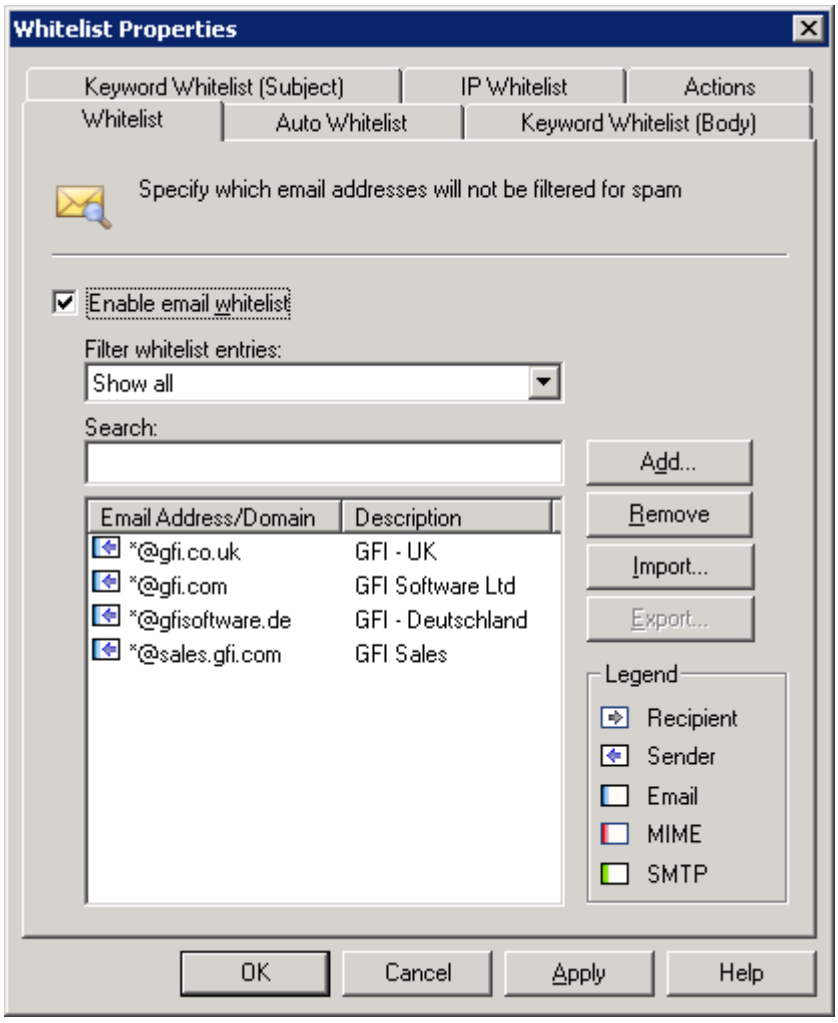
Important notes

1. Using the autowhitelist feature is highly recommended since this eliminates a high percentage of false positives.

2. In Keyword Whitelist it is recommended to add terms that spammers do not use and terms that relate to your nature of business, for example your product names. Entering too many keywords increases the possibility of emails not filtered by GFI MailEssentials and delivered to users' mailboxes.

Configuring Whitelist

1. Select **Anti-Spam ► Whitelist ► Properties**.



Screenshot 40 - Whitelisted domains

2. From the **Whitelist** tab, configure the email addresses and domains to whitelist. Select/Unselect **Enable email whitelist** to enable/disable whitelist. Configure the following whitelist options:

- **Add** - manually add email addresses, email domains (e.g. *@companysupport.com) or entire domain suffixes (e.g. *@*.edu) to the whitelist. Also specify the email header field to match for the emails to be whitelisted. You can also add a description to the entry in the **Description** field.

  NOTE: For more information about the difference between SMTP and MIME refer to:

  http://kbase.gfi.com/showarticle.asp?id=KBID002678

- **Remove** - select a whitelist entry and click **Remove** to delete.

- **Import** - import a list of whitelist entries from a file in XML format.

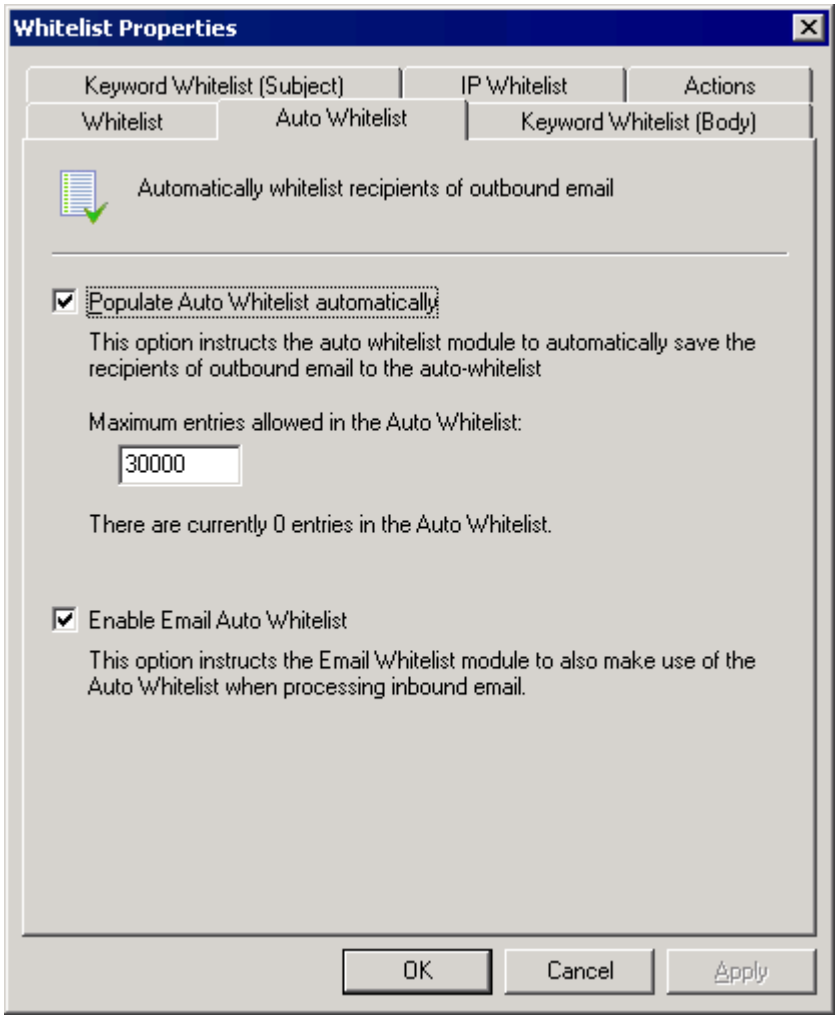
NOTE: A list of entries can be imported from a file in XML format in the same structure that GFI MailEssentials would export the list of entries.

» **Export** - export the list of whitelist entries to a file in XML format.

» **Filter whitelist entries** - from drop-down list select to filter the list of entries using the following criteria:

- **Show all** - Shows all entries in the whitelist
- **Show manually entered** - Shows the entries that were entered manually
- **Show automatically entered** - Shows the entries that were entered by the Auto Whitelist feature
- **Total entries per domain** - Displays a list of domains in the whitelist and the number of entries associated with that domain.

» **Search** - key in an entry to search for. Matching entries are filtered in the list of whitelist entries.


Whitelist Properties
Keyword Whitelist (Subject)
IP Whitelist
Actions
Whitelist
Auto Whitelist
Keyword Whitelist (Body)
Automatically whitelist recipients of outbound email
Populate Auto Whitelist automatically
This option instructs the auto whitelist module to automatically save the recipients of outbound email to the auto-whitelist
Maximum entries allowed in the Auto Whitelist:
30000
There are currently 0 entries in the Auto Whitelist.
Enable Email Auto Whitelist
This option instructs the Email Whitelist module to also make use of the Auto Whitelist when processing inbound email.
OK
Cancel
Apply

Screenshot 41 - Auto Whitelist options

5. Select the **Auto Whitelist** tab to configure the following options:

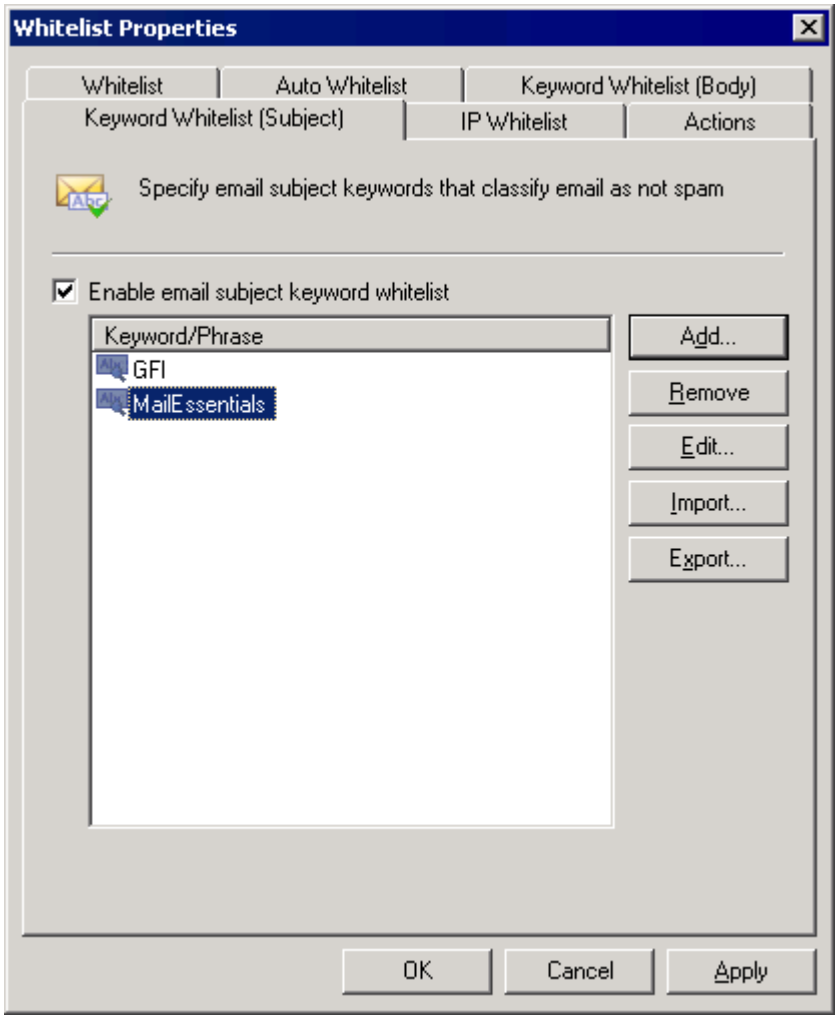
» **Populate Auto Whitelist automatically:** If this option is selected, the destination email addresses of outbound emails are automatically added to the whitelist

» **Maximum entries allowed in Auto Whitelist:** Specify the number entries allowed in Auto Whitelist. When the limit specified is exceeded, the oldest and least used entries are automatically replaced by the new entries.

NOTE: Entering a value larger than the default value of 30,000 can negatively affect the performance of GFI MailEssentials.

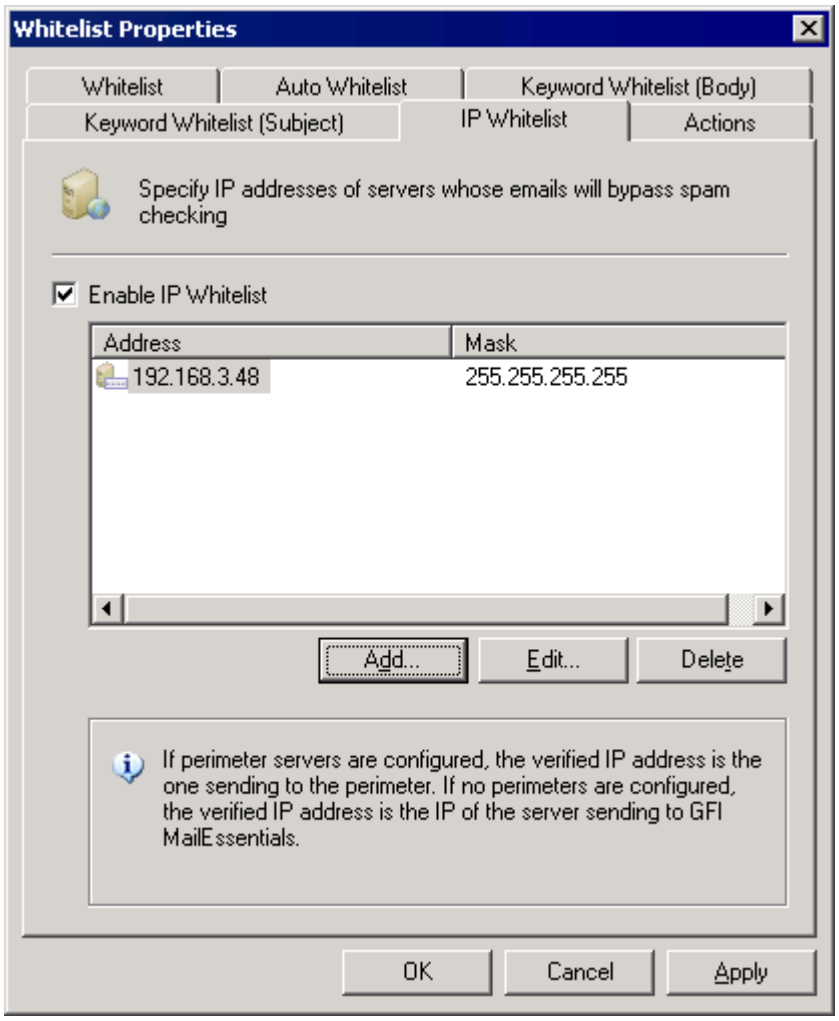
» **Enable Email Auto Whitelist:** If this option is selected, senders of incoming emails are matched against the auto whitelist. If the sender is present in the list, the email is forwarded directly to the recipient's Inbox.

NOTE: Auto whitelist entries can be viewed in the Whitelist tab by selecting the **Show automatically entered** option from the **Filter whitelist entries** dropdown.



Screenshot 42 - Whitelisting keywords

6. Select the **Keyword Whitelist (Subject)** or **Keyword Whitelist (Body)** tabs to specify keywords that flag emails as ham (valid email) and automatically allow the email to skip all anti-spam filtering. Specify new keywords by clicking **Add** button or use the **Remove**, **Edit**, **Import** and **Export** buttons to modify existing keywords.



Screenshot 43 - Whitelisting IPs

7. Select the **IP Whitelist** tab to allow emails received from specific IP addresses. Select **Enable IP Whitelist** to use this feature. Click **Add** to specify a single IP address or subnet/mask to bypass SPAM checks.

NOTE: When adding IP addresses to the IP Whitelist, you can also add a range of IP addresses using the CIDR notation.

8. Click **Actions** tab to enable / disable logging of whitelist occurrence to a file. Click **Browse** to specify a folder where to save logs.

9. Click **OK** to finalize your configuration.

New Senders filter

The New Senders filter enables GFI MailEssentials to automatically identify emails sent from senders to whom emails have never been sent before. Such senders are identified by referencing the data collected in the Whitelist.

Only emails in which no spam was detected and whose senders are not present in any Whitelist are delivered in the New Senders folder.

Since such emails could also be sent from legitimate users, these are collected in a dedicated folder. This makes these emails easily identifiable. Subsequently, these can be reviewed emails and any undetected spam added to the Email Blocklist.

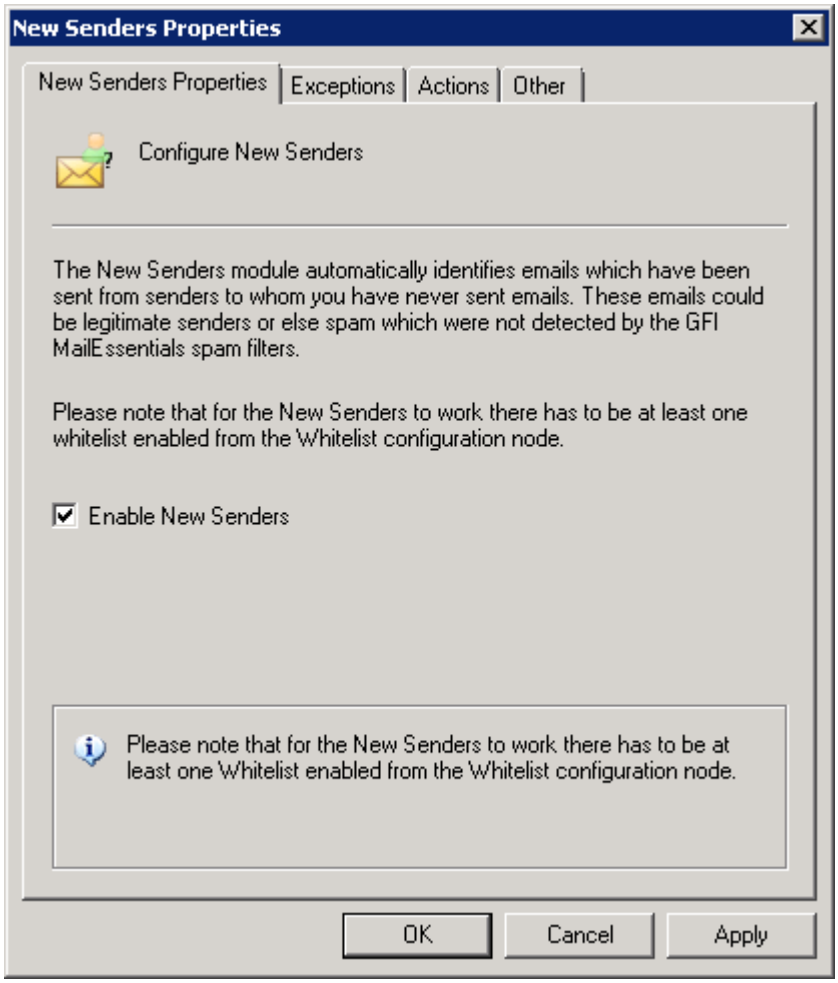
This filter is NOT enabled by default.

Important notes

1. Enable at least one of the available Whitelist to use the New Senders function. In the absence of the Whitelist functions (should no spam be detected by the other filters) received messages will be delivered to the recipient's Inbox. **ONLY** emails in which no spam was detected and whose senders are not present in the Whitelist are delivered in the New Senders folder.

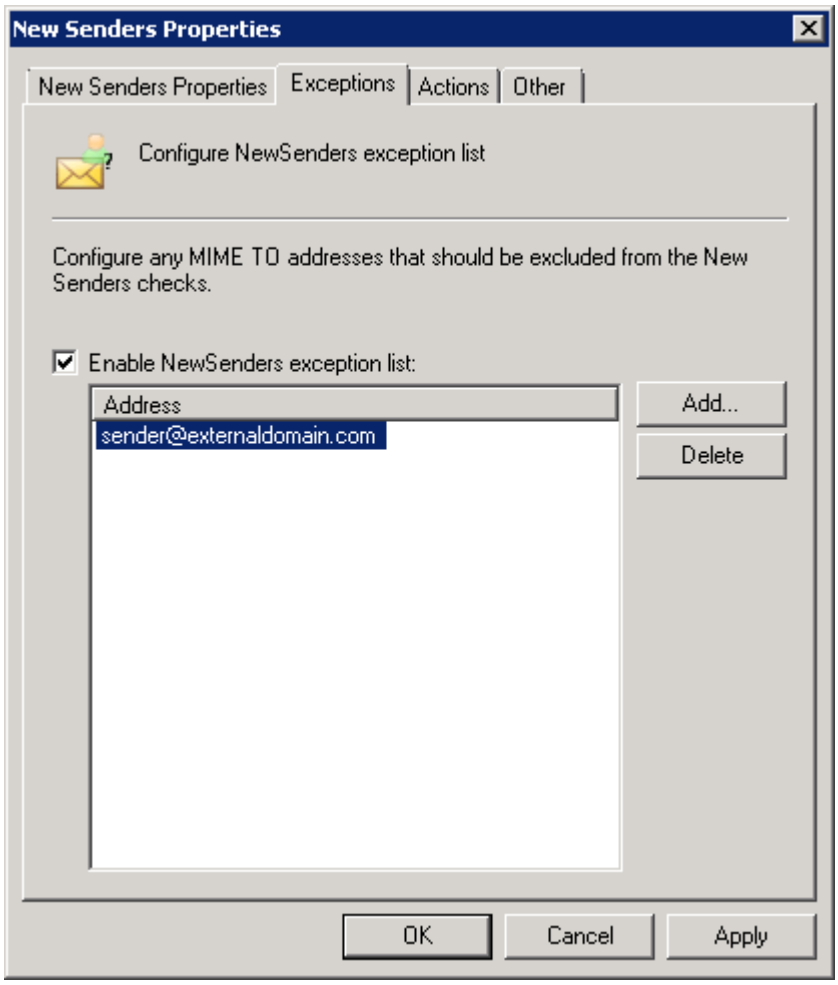
Configuring New Senders Filter

1. Select **Anti-Spam ► New Senders ► Properties**.


New Senders Properties
New Senders Properties
Exceptions
Actions
Other
Configure New Senders
The New Senders module automatically identifies emails which have been sent from senders to whom you have never sent emails. These emails could be legitimate senders or else spam which were not detected by the GFI MailEssentials spam filters.
Please note that for the New Senders to work there has to be at least one whitelist enabled from the Whitelist configuration node.
Enable New Senders
Please note that for the New Senders to work there has to be at least one Whitelist enabled from the Whitelist configuration node.
OK
Cancel
Apply

Screenshot 44 - New Senders properties

2. In the **New Senders Properties** tab, check the **Enable New Senders** checkbox to enable the check for new senders on all inbound messages and click on **Apply** button.



Screenshot 45 - New Senders Exception setup

3. Select **Exceptions** tab and check the **MIME TO exception list:** checkbox to configure local recipients whose emails are excluded from the New Senders check.

4. Click on **Add…** button and key in the email address of the sender.

» **Example:** administrator@master-domain.com.

Repeat for each address to add, and click **Apply** button to save.

NOTE: To temporarily disable your exception list, do not delete all address entries made, but uncheck the **MIME TO exception list:** checkbox.

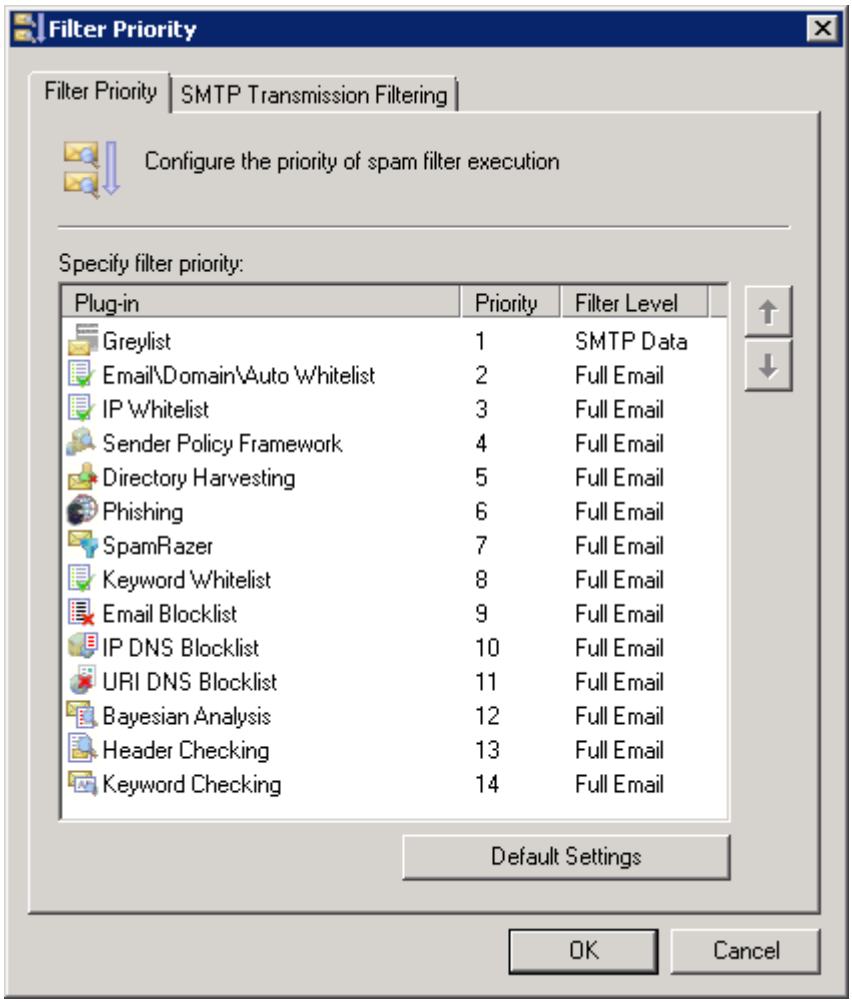
5. Click **Actions** tab to select the actions to perform on messages identified as spam. For information on the actions to perform refer to the **Spam Actions - What to do with spam email** section in this manual.

6. Click **OK** to finalize setup

Sorting anti-spam filters by priority

In GFI MailEssentials, the order in which the anti-spam checks are applied to inbound messages can be customized.

NOTE: The order of all available filters can be customized except for the New Senders filter, which is always automatically set to the lowest priority. This is due to its dependency on the results of the Whitelist checks and the other anti-spam filters.



Screenshot 46 - Assigning filter Priorities

1. Right click **Anti-Spam ► Filter Priority** node and select **Properties**.

2. Select a filter and click on the (up) button to assign a higher priority to the selected filter or click on the (down) button to assign a lower priority to the selected filter.

NOTE: Click **Default Settings** to restore the filter order to the default order.

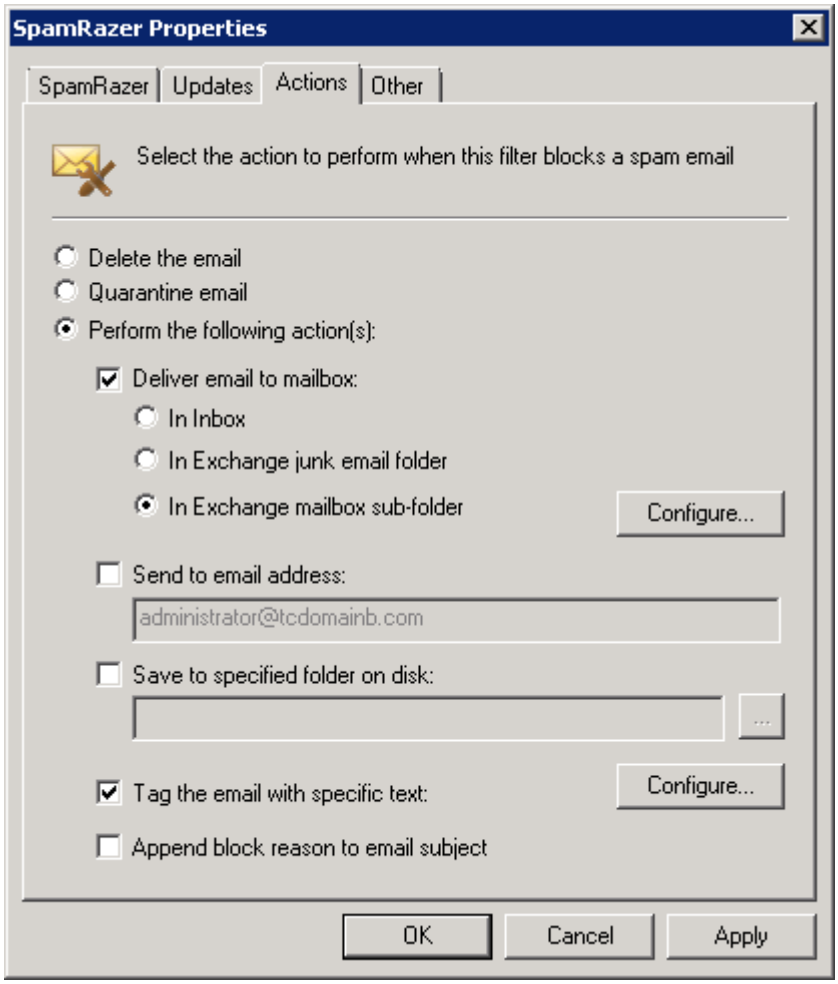
3. Click **OK** to finalize your configuration. Changes take effect immediately.

5.2 Spam Actions - What to do with spam email

The **Actions** tab in the Anti-Spam filter dialogs define what should be done with emails marked as spam. Different actions can be defined for each of the spam filters.

» **Example:** Delete emails detected by SpamRazer filter, but do not delete emails marked as spam by the Keyword Checking filter.

Configuring Spam Actions



Screenshot 47 - Configuring the action that should be taken

1. In the **Actions** tab, select an option that defines which action to take on emails marked as spam:

» **Delete the email** - Delete an email which is blocked by that particular spam filter. Other spam actions are disabled if the email is deleted.

» **Quarantine email** - Emails detected as spam will be stored in the Quarantine Store. Other spam actions are disabled if the email is quarantined. For more information refer to **Using Quarantine** chapter.

» **Deliver email to mailbox** - choose the folder where to deliver the email:

- **In Inbox** - Use this option to route spam to the user's Inbox.
- **In Exchange junk email folder** - Use this option to route all spam to the user's default Junk E-mail folder
- **In Exchange mailbox sub-folder -** Use this option to route all spam to a specific folder in the user's mailbox. Click **Configure** to launch the Move to Exchange folder dialog and type the folder where to move spam email.
  - **Example 1:** Type **Suspected Spam** for a custom folder to be created in the same level of the Inbox folder.
  - **Example 2:** Type **Inbox\Suspected Spam** for a custom folder to be created in the Inbox folder.

NOTE 1: This option requires that:

- GFI MailEssentials is installed on the Microsoft Exchange Server machine. If GFI MailEssentials is not installed on the Microsoft Exchange Server, refer to the **Moving spam email to user's mailbox folders** chapter in this manual.

- Active Directory mode is enabled.
- The mail server is Microsoft Exchange Server 2003 or Microsoft Exchange Server 2007/2010 with the Mailbox Server Role present.

NOTE 2: For Microsoft Exchange 2010 a dedicated user is required to enable this option. In the Actions dialog click **Configure** and click **Specify user account** to specify the dedicated user. In the Move to Exchange configuration dialog, select one of the following options:

- **Move spam using an automatically created user** - Select this option to let GFI MailEssentials automatically create a user with all the required rights.
- **Move spam using the following user account** - Select this option to use a manually created user. Specify the credentials (Domain\username and password) of a dedicated user and click **Set impersonation rights** to assign the required rights to the specified user.

  NOTE: The manually specified user credentials must be dedicated to this feature only. The username, password or other properties must not be changed from Microsoft Exchange or Active Directory, otherwise the Move to Exchange folder feature will not work.

» **Send to email address** - Send email identified as spam to a specific email address.

- **Example:** An email address of a public folder. This way someone can be assigned to periodically check email marked as spam, and identify email that might have been wrongly marked as spam.

The subject of the email will be in the format: **[recipient] [subject]**

» **Save to specified folder on disk** - Saves email detected as spam to the path specified,

- **Example:** 'C:\Spam'.

The file name of the saved email is in the following format:

`[Sender_recipient_subject_number_.eml]` (for example: `C:\Spam\jim@comp.com_bob@comp.com_MailOffers_1_.eml`)

» **Tag the email with specific text** - Select this option to add a tag to the email subject. Click **Configure** to modify tagging options. In the Tag Email dialog, key in the text to use for tagging and specify where to place the tag:

- **Prepend to subject** - to insert the specified tag at the start (i.e. as a prefix) of the email subject text.
  - **Example:** '[SPAM]Free Web Mail'.
- **Append to subject** - to insert the specified tag at the end (i.e. as a suffix) of the email subject text.
  - **Example:** 'Free Web Mail[SPAM])'.
- **Add tag in an X-header…** - to add the specified tag as a new X-header to the email. In this case, the X-Header will have the following format :

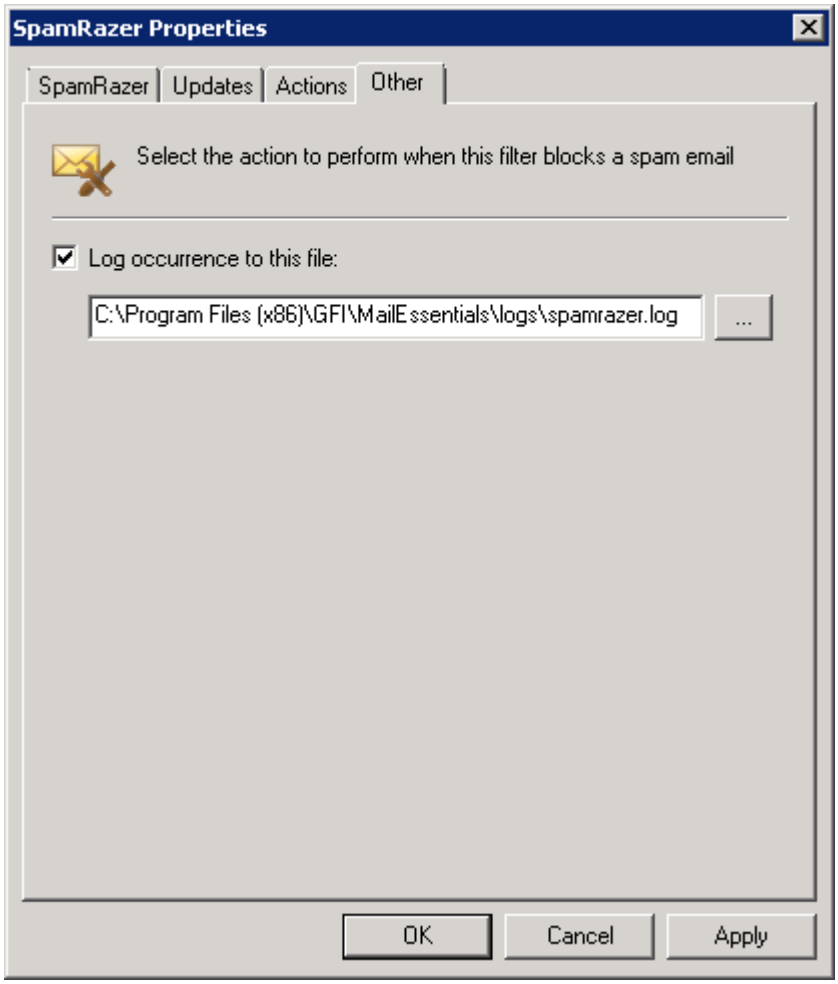
  ```
  X-GFIME-SPAM: [TAG TEXT]
  X-GFIME-SPAM-REASON: [REASON]
  ```

  - **Example**:

    ```
    X-GFIME-SPAM: [This is SPAM]
    X-GFIME-SPAM-REASON: [IP DNS Blocklist Check failed - Sent from Blocklisted Domain]
    ```

» **Append block reason to email subject -** If this option is enabled, the name of the filter which blocked the email and the reason for blocking are appended to the subject of the blocked email.

Other options



Screenshot 48 - The other actions tab

Select the **Other** tab, to specify a number of optional actions:

» **Log occurrence to this file -** Log the spam email occurrence to a log file of your choice.

NOTE: Log files may become very large. GFI MailEssentials enables log rotation, where new log files are created periodically or when the log file reaches a specific size. To enable log file rotation navigate to **Anti-Spam ► Anti-Spam Settings**. Select **Anti-spam logging** tab and check **Enable log file rotation**. Specify the rotation condition by time or file size.

NOTE: When the GFI MailEssentials installation is an upgrade from version 14 or less that used the fake Non Delivery Report (NDR) action, the option to create a fake NDR is retained. This feature is not included in GFI MailEssentials 2010 since it can be a threat to the mail flow system. For more information about sending fake NDRs refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID002898

Anti-spam global actions

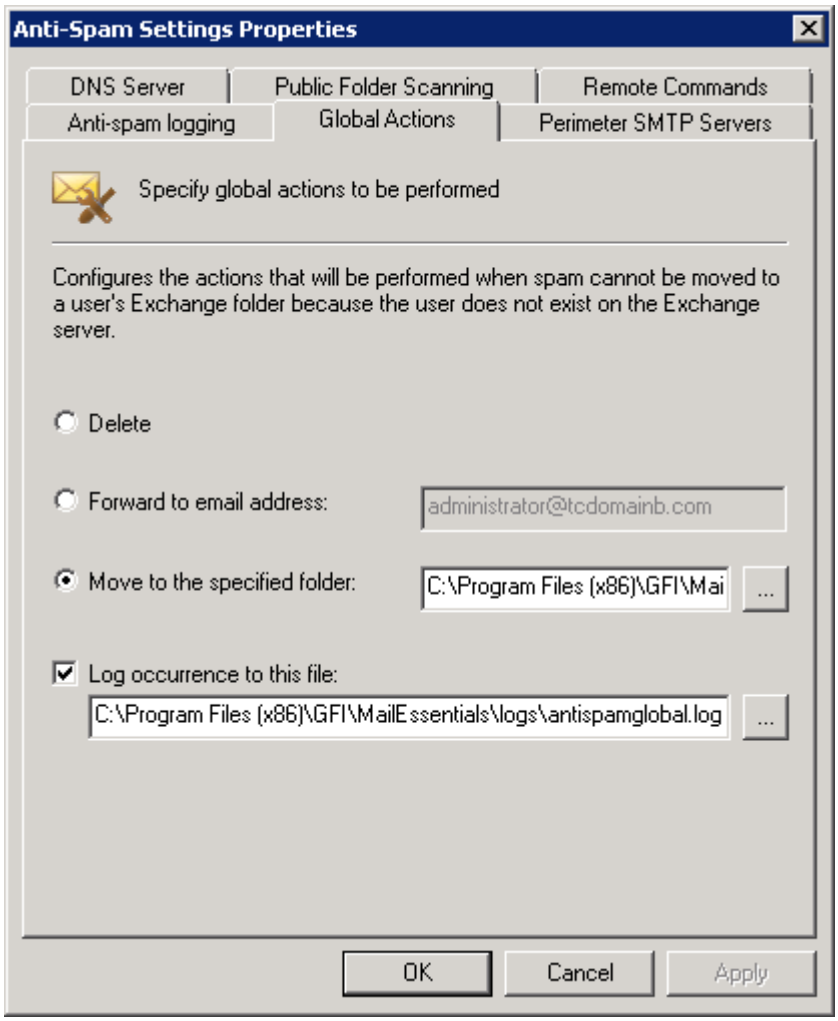
A lot of spam is sent to email addresses that no longer exist. Generally, these emails are simply deleted however for troubleshooting or evaluation purposes, you might want to move these emails to a folder or forward them to a particular email address.

NOTE: This section applies only for installations on Microsoft Exchange Server that have the **Move to subfolder of user's mailbox** enabled. Refer to the **Spam Actions - What to do with spam email** section in this manual for more information how to enable this feature.

On other servers, the anti-spam global actions tab will not appear.

Configuring Anti-spam global actions

1. Right click **Anti-Spam ► Anti-Spam Settings** node and select **Properties**.



Screenshot 49 - Global actions

2. Select **Global Actions** tab and choose whether to:

- Delete the email
- Forward it to an email address
- Move it to a specified folder.

3. Select the **Log occurrence to this file** to log spam to a log file.

5.3 Configuring Quarantine

The GFI MailEssentials Quarantine feature provides a central store where all inbound emails detected as spam are retained for a number of days. This ensures that users do not receive spam in their mailbox and processing on the mail server is reduced.

Administrators and mail users can review quarantined emails by accessing the quarantine interface from a web browser. GFI MailEssentials can also send regular email reports to email users to review their blocked emails.

Important Notes

1. To quarantine spam, change the anti-spam filters actions to **Quarantine email**. For more information refer to **Spam Actions - What to do with spam email**.

2. The GFI MailEssentials Quarantine Store requires disk space to retain the organization's spam emails for a number of days. The amount of disk space required depends on:

- the quantity of spam received
- how long spam is retained in the Quarantine Store.

On average, 100,000 spam emails of 5KB each will require approximately 600MB of disk space to

store the email and its metadata.

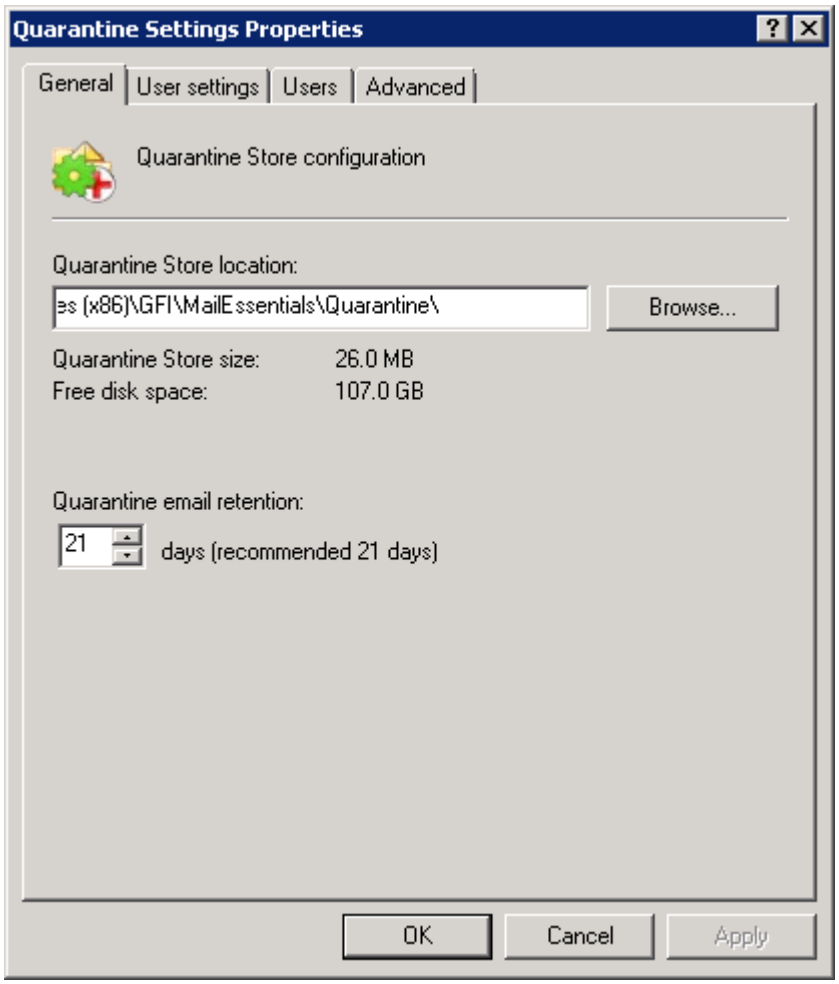
3. If the free disk space where the Quarantine Store is saved is 512MB or less, GFI MailEssentials stops quarantining spam. Spam will be tagged and delivered to recipients' mailboxes until free disk space increases to more than 512MB. This ensures that the disk will not run out of space.

4. The GFI MailEssentials quarantine feature requires the Microsoft IIS WWW service.

5.3.1 Configuring Quarantine

1. Launch GFI MailEssentials configuration console by clicking **Start ► Programs ► GFI MailEssentials ► GFI MailEssentials Configuration**.

2. Right click **Anti-Spam ► Quarantine ► Quarantine Settings** and click **Properties**.



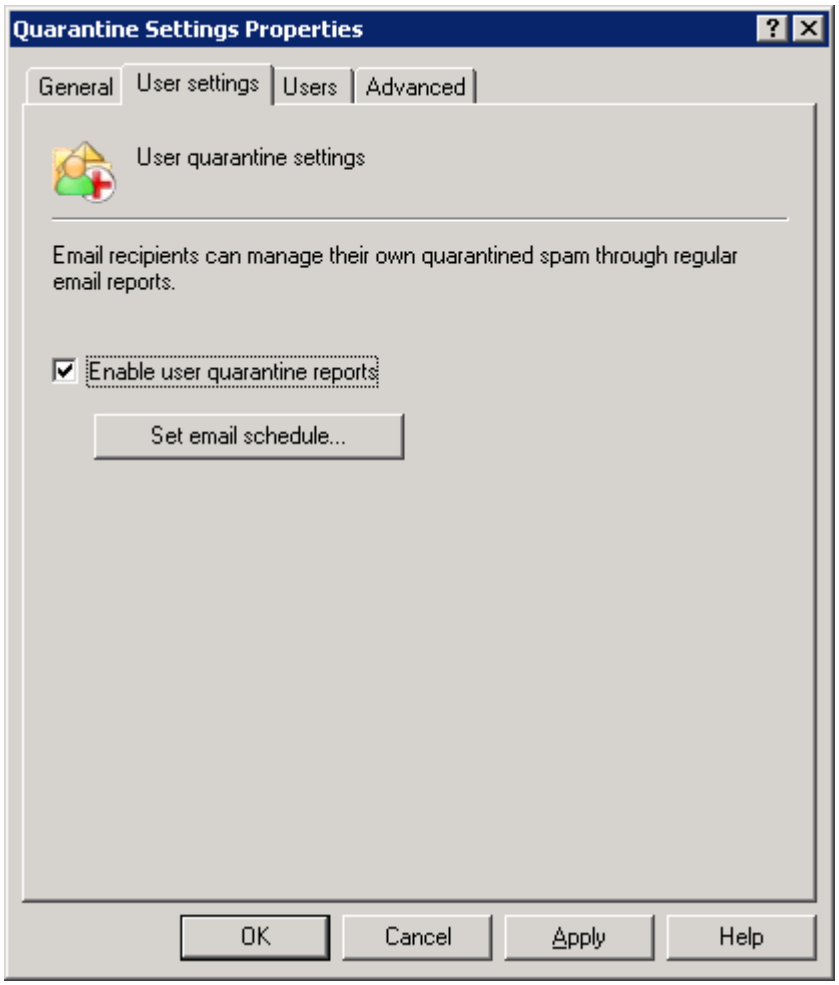
Screenshot 50 - Quarantine settings

3. From the **General** tab configure:

- **Quarantine Store location** - Click **Browse** to specify the path where to save the Quarantine Store. The default path is *<GFI MailEssentials installation folder path>\Quarantine*.

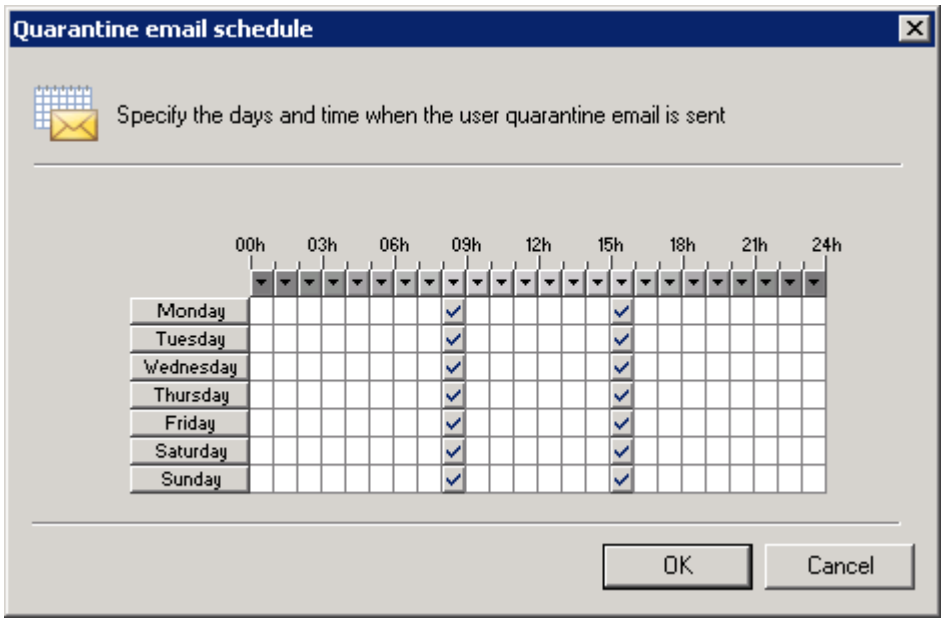
  IMPORTANT: Ensure that the disk partition where the Quarantine Store is saved has sufficient disk space. Spam emails will not be quarantined if the free disk space is less than 512MB. On reaching 512MB, email quarantine operation will stop and spam will be tagged and delivered to recipients' mailboxes until free disk space increases to more than 512MB.

- **Quarantine email retention period** - Specify the number of days to retain spam in Quarantine Store.



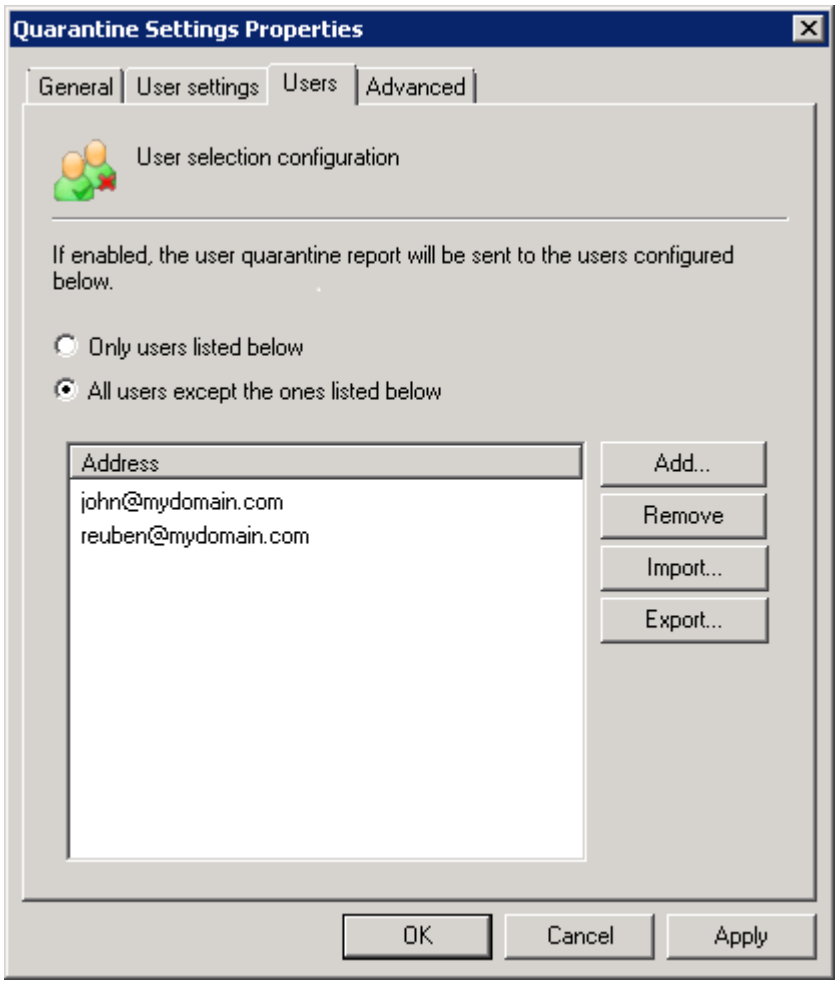
Screenshot 51 - User settings

4. User quarantine reports are regular emails sent to mail users containing a list of blocked emails. Users can review this list to check and approve any legitimate emails that were blocked. To enable email reports, select **User Settings** tab and select **Enable user quarantine reports**.



Screenshot 52 - Quarantine email schedule

5. Click **Set email schedule…** to specify the weekdays and time when to send the quarantine email report. Click **OK** to apply schedule.



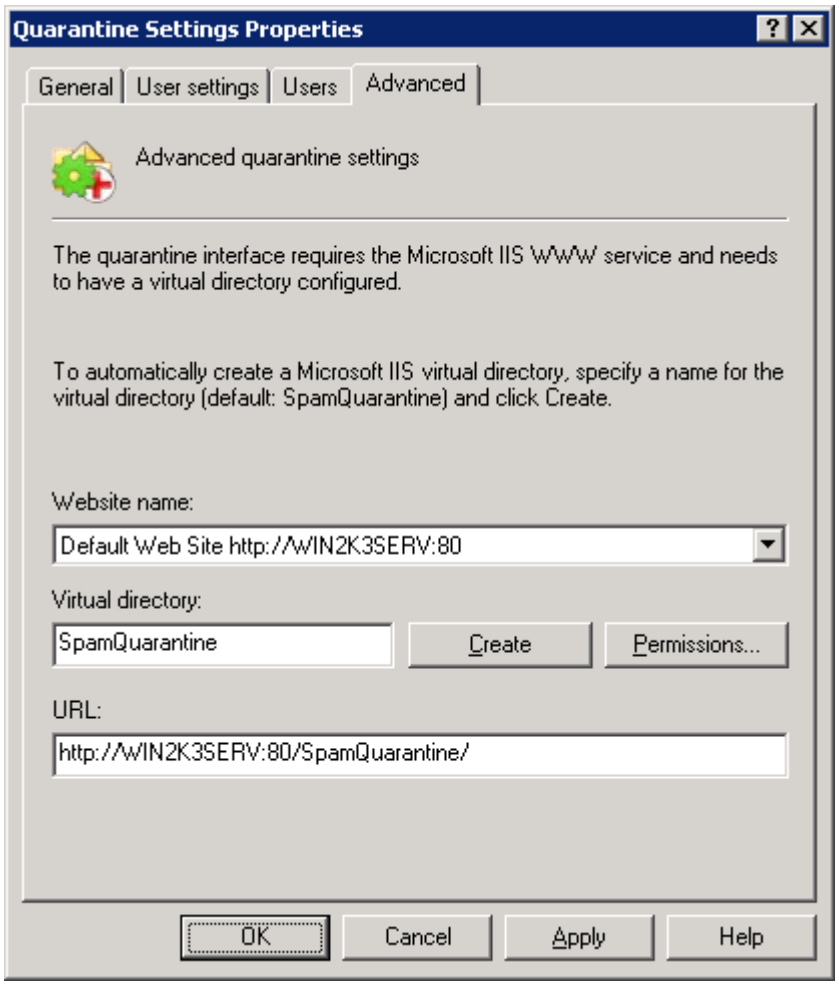
Screenshot 53 - Selecting the users to receive the quarantine email reports

6. When enabling quarantine email reports, navigate to the **Users** tab and specify the users to receive the quarantine reports. Select:

- **Only users listed below** - only the users specified in the list will receive the quarantine email reports.
- **All users except the ones listed below** - all email users will receive the quarantine email reports except for the users specified in the list.

7. Depending on the selection made in step 7, specify the email addresses to add to the list. Click:

- **Add** - manually type an email address to add to the list
- **Remove** - select the users to remove from the list and click **Remove**
- **Import** - import a list of email addresses from a .xml file
- **Export** - export the list of email addresses to a .xml file.



Screenshot 54 - Configuring advanced quarantine settings

8. Click **Advanced** tab to configure advanced settings. Configure:

- **Website name** - select the website to use to access the quarantine web interface.
- **Virtual directory** - type a name for the virtual directory and click **Create** to automatically create the virtual directory. The default name is 'SpamQuarantine'.
- **Permissions…** - launches a separate dialog to specify the users or groups that are allowed full access to all quarantined emails.
- **URL** - (Optional) The default URL used in quarantine user reports to access the quarantine interface. This is defined in the following format:

  `http://<web server name>/<virtual directory>`

  This URL, however, is not accessible over the internet. If a public domain is available, you can manually change the web server name to a public domain that is accessible over the Internet. Links in the user quarantine email reports will now use this URL.

For information how to use Quarantine, refer to **Using Quarantine**.

5.4 Public folder scanning

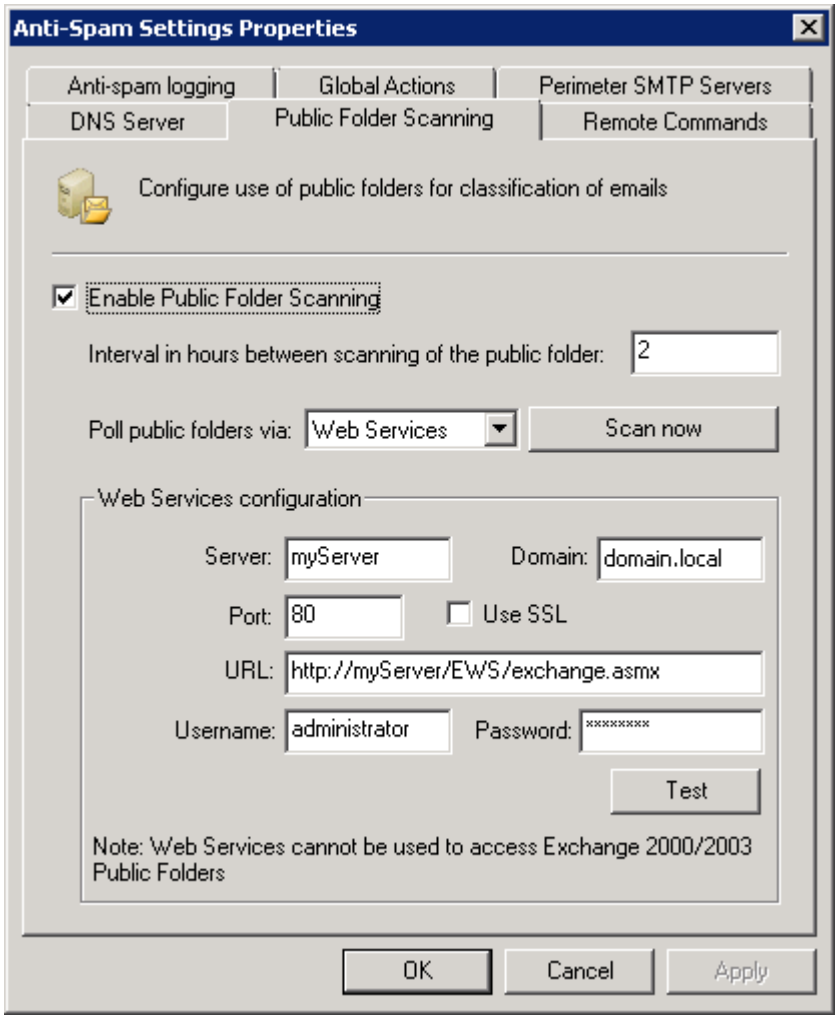
Spamming techniques are continuously evolving and consequently you might encounter instances when spam still makes it through anti-spam filters on to the recipient's Inbox. Through public folder scanning, users can manually classify email as spam and 'teach' GFI MailEssentials spam patterns to classify similar email as spam.

Public folder scanning enables GFI MailEssentials to retrieve emails from public folders to add to whitelist/blocklist and HAM/SPAM databases. On systems running Microsoft Exchange Server or Lotus Domino, public folders are created automatically on completion of the configuration process.

To enable public folders scanning follow the instructions listed in the sections below.

5.4.1 Public folder scanning setup for Microsoft Exchange Servers

1. From the GFI MailEssentials configuration console right click the **Anti-spam ► Anti-Spam Settings** and select **Properties**.



Screenshot 55 - Configuring Public folder scanning

2. Select **Public Folder Scanning** tab, and click on **Enable Public Folder Scanning** checkbox.

3. From the **Poll public folders via** list select the method GFI MailEssentials uses to retrieve emails from public folders.

- **Exchange Server 2003** - Select MAPI, IMAP or WebDAV.
- **Exchange Server 2007** - Choose WebDAV or Web Services.
- **Exchange Server 2010** - Choose Web Services.

Available options are:

- **MAPI** - To use MAPI, GFI MailEssentials must be installed on the machine on which Microsoft Exchange Server is installed. No other settings are required.
- **IMAP** - Requires Microsoft Exchange IMAP service. IMAP enables remote scanning of public folders and works well in environments running firewalls. In addition, IMAP can be used with other Mail servers that support IMAP. Parameters required are:
  - Mail server name
  - Port number (default IMAP port is 143)
  - Username/password

- Select the **Use SSL** option to use a secure connection

» **WebDAV** - Specify Mail server name, port (default WebDAV port is 80), username/password and domain. To use a secure connection select the **Use SSL** checkbox. By default, public folders are accessible under the 'public' virtual directory. If this has been changed, specify the correct virtual directory name to access the public folders by editing the text in the **URL** box.

» **Web Services** - Specify the following details:

- **Server** - mail server name
- **Domain** - use the local domain

  NOTE: If both a local and a public domain exist, always use the local domain.
- **Port** - default Web Services port (80, or 443 if using SSL).
- **Username/password** - use credentials with administrative privileges or create a dedicated user from Microsoft Exchange Management Shell by entering the following command to add the appropriate permissions:

  ```
  Add-ADPermission -identity "Mailbox Store" -User NewUser -
  AccessRights GenericALL
  ```

  NOTE: Replace '`Mailbox Store`' with the name of the mailbox store that contains the user mailboxes and '`NewUser`' with the username of the created user.
- **Use SSL** - Select this option if Exchange Web Services require a secure connection. By default, Web Services requires SSL.
- **URL** - By default, public folders are accessible under the 'EWS/exchange.asmx' virtual directory. If this has been changed, specify the correct virtual directory name to access the public folders by editing the text in the URL box.

NOTE: It is recommended to test the settings manually, by loading the URL in a web browser. This should load an XML formatted file, named **services.wsdl**.

4. Click **Scan Now** to automatically create Public folders.

5. Click **Test** if you are setting up IMAP, WebDAV or Web Services. On screen notification will confirm success/failure. If the test fails, verify/update credentials and re-test.

5.4.2 Configure a dedicated user account for Exchange Server 2003

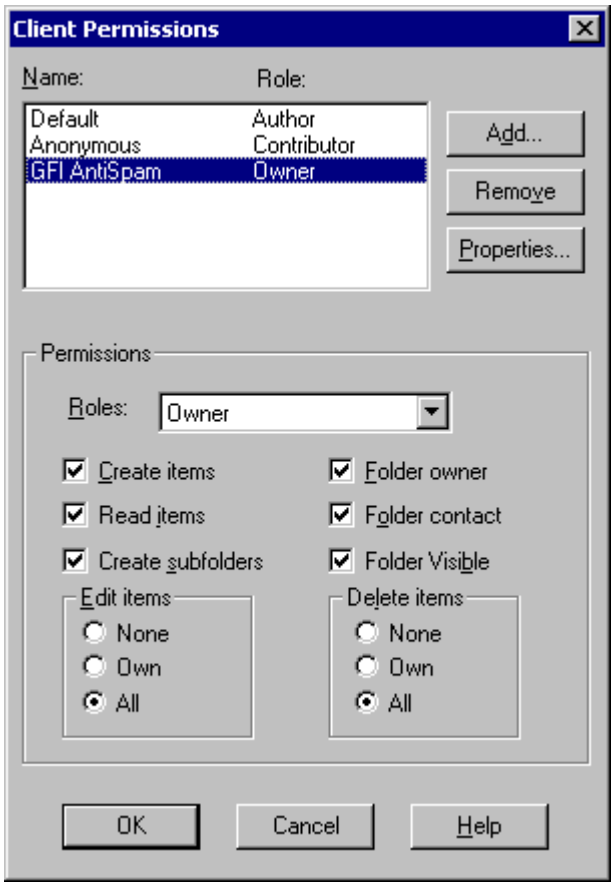
When GFI MailEssentials is installed in a DMZ, it is highly recommended that for security reasons a dedicated user account is created to retrieve/scan email from public folders. Users will have access to the GFI AntiSpam folders.

1. Create a new Active Directory (AD) user with power user privileges.

2. From the Microsoft Exchange System Manager, expand **Folders ► Public Folders** node.

3. Right click **GFI AntiSpam Folders** public folder and select **Properties**.

4. Click **Permissions** tab and select **Client permissions**.



Screenshot 56 - Setting user role

5. Click **Add…**, select new user, and click **OK**.

6. Select new user from the client permissions list and from provided list set its role to 'Owner'. Ensure that all checkboxes are selected and the radio buttons are set to **All**.

7. Click **OK** to finalize your configuration.

8. From the Microsoft Exchange System Manager right click **GFI AntiSpam Folders** and select **All tasks ► Propagate settings**.

NOTE: For Microsoft Exchange Server 2003 SP2, right click **GFI AntiSpam Folders** and select **All tasks ► Manage Settings** option.

9. Select the **Folder rights** or **Modify client permissions** option and click **OK** or **Next**.

10. Specify the credentials of power user account created in step 1 and test the setup to ensure the permissions are correct.

5.4.3 Configure a dedicated user account for Exchange Server 2007/2010

When configuring a dedicated user account to retrieve the emails from the GFI AntiSpam Public folders, the user would need to have 'owner' access rights on the GFI AntiSpam Public Folders.

1. Create a new Active Directory (AD) (power) user.

2. Logon to the Microsoft Exchange Server using administrative privileges.

3. Open 'Microsoft Exchange Management Shell' and key in following command:

```
Get-PublicFolder -Identity "\GFI AntiSpam Folders" -Recurse | ForEach-
Object {Add-PublicFolderClientPermission -Identity $_.Identity -User
"USERNAME" -AccessRights owner -Server "SERVERNAME"}
```

Change "USERNAME" and "SERVERNAME" to the relevant details of the Active Directory user in question.

» Example:

```
Get-PublicFolder -Identity "\GFI AntiSpam Folders" -Recurse |
ForEach-Object {Add-PublicFolderClientPermission -Identity
$_.Identity -User "mesuser" -AccessRights owner -Server "exch07"}
```

5.4.4 Hiding user posts in GFI AntiSpam Folders

For privacy and security purposes, it is highly recommended that you hide user posts made on GFI AntiSpam folders. This way, users will only be able to post to the folders without viewing existing posts (not even the ones they posted themselves). To configure user privileges and hide posts for unauthorized users do as follows:

Microsoft Exchange 2003

1. From the Microsoft Exchange System Manager expand **Folders ► Public Folders** node.

2. Right click **GFI AntiSpam Folders** public folder and select **Properties**.

3. Select the **Permissions** tab and click **Client permissions**.

4. Click **Add…**, and select the user/group to hide the posts from and click **OK**.

5. Select user/group configured earlier to the client permissions list and set its role to **Contributor**.

6. Ensure that only the **Create items** checkbox is selected and the radio buttons are set to **None**.

7. Click **OK** to finalize your configuration.

8. From the Microsoft Exchange System Manager right click **GFI AntiSpam Folders** and select **All tasks ► Propagate settings**.

9. Select **Folder rights** checkbox and click **OK**.

Microsoft Exchange 2007

1. From Microsoft Exchange Management Shell, key in the following command:

```
ReplaceUserPermissionOnPFRecursive.ps1 -Server "server" -TopPublicFolder
"\'GFI AntiSpam Folders'" -User "Default" -Permissions Contributor
```

Replace “server” with the full computer name.

2. When prompted, key in **y** to confirm permissions for each folder.

This command will set the default permissions for the GFI MailEssentials Public Folders to contributor, where users can move emails to the Public Folders but cannot view or modify entries. By default administrators are owners of the Public Folders and can view or modify entries. For more information about Public Folders permissions refer to:

http://technet.microsoft.com/en-us/library/bb310789.aspx

Microsoft Exchange 2010

1. From Microsoft Exchange Management Shell, change the folder to the Microsoft Exchange scripts folder that can be found in the Microsoft Exchange installation folder. If Microsoft Exchange is installed in the default path, the scripts folder is stored in:

C:\Program Files\Microsoft\Exchange Server\V14\Scripts\

2. Key in the following command:

```
ReplaceUserPermissionOnPFRecursive.ps1 -Server "server" -TopPublicFolder
"\GFI AntiSpam Folders" -User "Default" -Permissions Contributor
```

Replace “server” with the full computer name.

This command will set the default permissions for the GFI MailEssentials Public Folders to contributor, where users can move emails to the Public Folders but cannot view or modify entries. By default administrators are owners of the Public Folders and can view or modify entries. For more information about Public Folders permissions refer to:

http://technet.microsoft.com/en-us/library/bb310789(EXCHG.140).aspx

5.4.5 Public folder scanning setup for Lotus Domino servers

Step 1: Create a new database which used to store GFI MailEssentials Public folders.

1. From the IBM Domino Administrator, click on **File ► Database ► New**.

2. Key in the following details for the new database:

   - Server: <Your Domino Server details>
   - Title: Public-Folder
   - File name: Public-F.nsf
   - Select 'Mail (R7)' as the template for the new Database

3. Click **OK** to create the database.

Step 2: Convert the database format of the newly created database.

1. From the Lotus Domino server Console, run the following command:

```
Load Convert -e -h <Database Filename>
```

   - Example:

     ```
     Load Convert -e -h Public-F.nsf
     ```

Step 3: Create a new Mail-In database:

A new mailbox needs to be created in order to store the new GFI MailEssentials Public Folder.

1. From the IBM Domino Administrator, select **People & groups** tab and click on **Mail-In Databases and Resources**.

2. Click **Add Mail-In Database** and key in the New Mail-In Database as follows:

   - Mail-in name: Public Folders
   - Description: The GFI MailEssentials Mailbox
   - Internet address: <public@<yourdomain.com>
   - Internet Message: 'No Preference'
   - Encrypt incoming mail: 'No'
   - Domain: <yourdomain>
   - Server: <Your Domino server name>
   - File name: 'Public-F.nsf'

NOTE: You will need to associate a user with the Mail-In-database created above. This account will be used by the GFI MailEssentials server to connect to the Lotus Domino Server.

Step 4: Configure GFI MailEssentials

Define the shared namespace which will be used when connecting to the Lotus Domino IMAP service:

1. Click **Start ► Run** and type **Regedit**.

2. Locate the following Registry Key:

```
<HKEY_LOCAL_MACHINE\SOFTWARE\GFI\ME15\Attendant\rpfolders:8\>
```

3. Create the following Keys:

Name: 'FolderDelimiter'	Name: 'SharedNamespace'
Type: STRING	Type: STRING
Value: '\\'	Value: <*Public Folder Prefix\Name of new Mail-In Database*\>

Get the values for the 'sharednamespace' key as follows:

Public folder prefix name

1. From the IBM Domino Administrator, click **Configuration** Tab.

2. Expand **Server ► Configurations,** click on your Domino Server and click **Edit Configuration**.

3.From the **IMAP** tab, select **Public and Other Users' Folders** tab. The 'Public Folder Prefix' can be found under the Public Folder Section.

Mail-In database name

1. From the IBM Domino Administrator select **People & Groups** tab.

2. Click on **Mail-In Databases and Resources** node. Name of the New Mail-In Database is listed within the right pane.

Step 5: Restart the IMAP Service on the Domino Server

1. Open the Lotus Notes Console

2. Type 'tell imap quit' and wait until the task completes.

3. Once the above is complete, type 'load imap'

Step 6: Configure GFI MailEssentials

Configure the GFI MailEssentials Public Folder Scanning properties. 1. From the GFI MailEssentials Configuration, right click **Anti Spam** Node and select **Properties.**

2. Select **Public Folder Scanning** tab and key in the following values:

- Server: <IP Address of Domino Server>
- Port: 143 (default)
- Username: Username associated with the mail-in database
- Password: User password

3. Test configuration by clicking **Test** button and click **Scan now** to generate the public folders.

Step 7: Ensure the Public Folders are created

Using telnet to determine if Public folders were created successfully:

1. From the GFI MailEssentials machine load up command prompt.

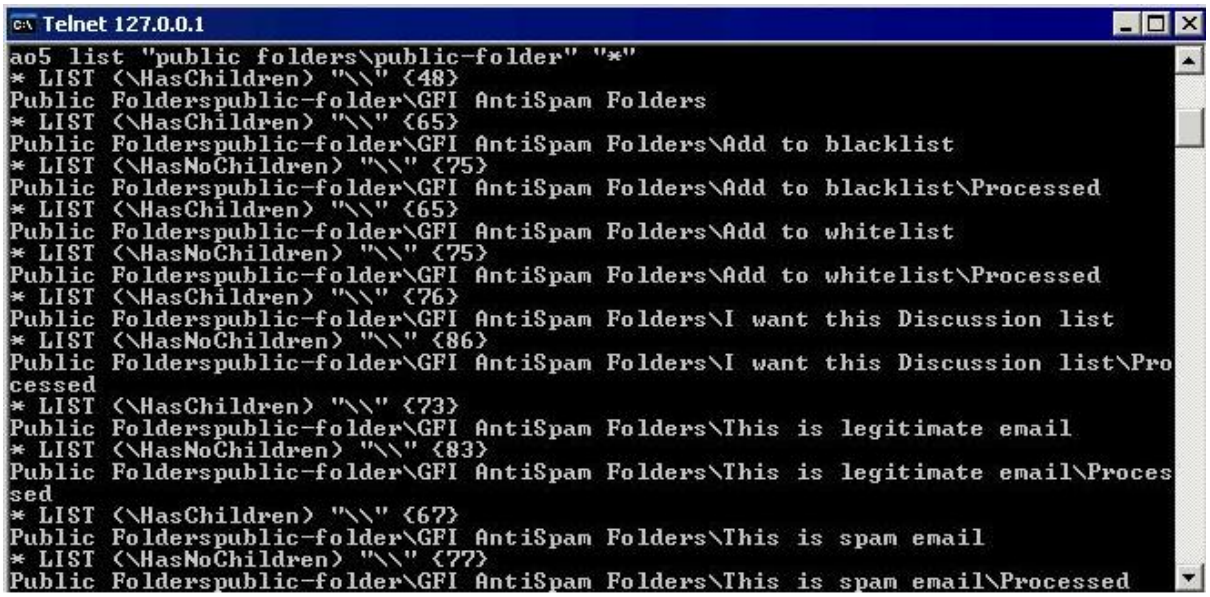
2. Type 'telnet'

3. Type 'Open <*IP ADDRESS*> 143'

4. Type 'ao1 login <public@yourdomain.com> <password>'

5. Type 'ao5 list "<Public Folder Prefix\Name of new Mail-In Database\>" "*"

6. The output of the above command should show the public folders as in the following screenshot:


Telnet 127.0.0.1
ao5 list "public folders\public-folder" "*"
* LIST (\HasChildren) "\\" {48}
Public Folderspublic-folder\GFI AntiSpam Folders
* LIST (\HasChildren) "\\" {65}
Public Folderspublic-folder\GFI AntiSpam Folders\Add to blacklist
* LIST (\HasNoChildren) "\\" {75}
Public Folderspublic-folder\GFI AntiSpam Folders\Add to blacklist\Processed
* LIST (\HasChildren) "\\" {65}
Public Folderspublic-folder\GFI AntiSpam Folders\Add to whitelist
* LIST (\HasNoChildren) "\\" {75}
Public Folderspublic-folder\GFI AntiSpam Folders\Add to whitelist\Processed
* LIST (\HasChildren) "\\" {76}
Public Folderspublic-folder\GFI AntiSpam Folders\I want this Discussion list
* LIST (\HasNoChildren) "\\" {86}
Public Folderspublic-folder\GFI AntiSpam Folders\I want this Discussion list\Pro
cessed
* LIST (\HasChildren) "\\" {73}
Public Folderspublic-folder\GFI AntiSpam Folders\This is legitimate email
* LIST (\HasNoChildren) "\\" {83}
Public Folderspublic-folder\GFI AntiSpam Folders\This is legitimate email\Proces
sed
* LIST (\HasChildren) "\\" {67}
Public Folderspublic-folder\GFI AntiSpam Folders\This is spam email
* LIST (\HasNoChildren) "\\" {77}
Public Folderspublic-folder\GFI AntiSpam Folders\This is spam email\Processed

7. Type ‘ao3 logout’

NOTE: Use the Lotus notes designer to remove any unwanted views and forms from the database created previously.

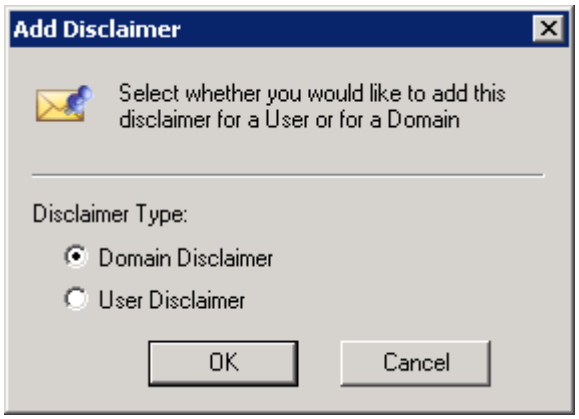
6 Customizing other features

6.1 Disclaimers

Disclaimers are standard text added to the bottom or top of outbound email for legal and/or marketing reasons. These assist companies in protecting themselves from potential legal threats resulting from the contents of an email and to add descriptions about the products/services offered.

6.1.1 Configuring disclaimers

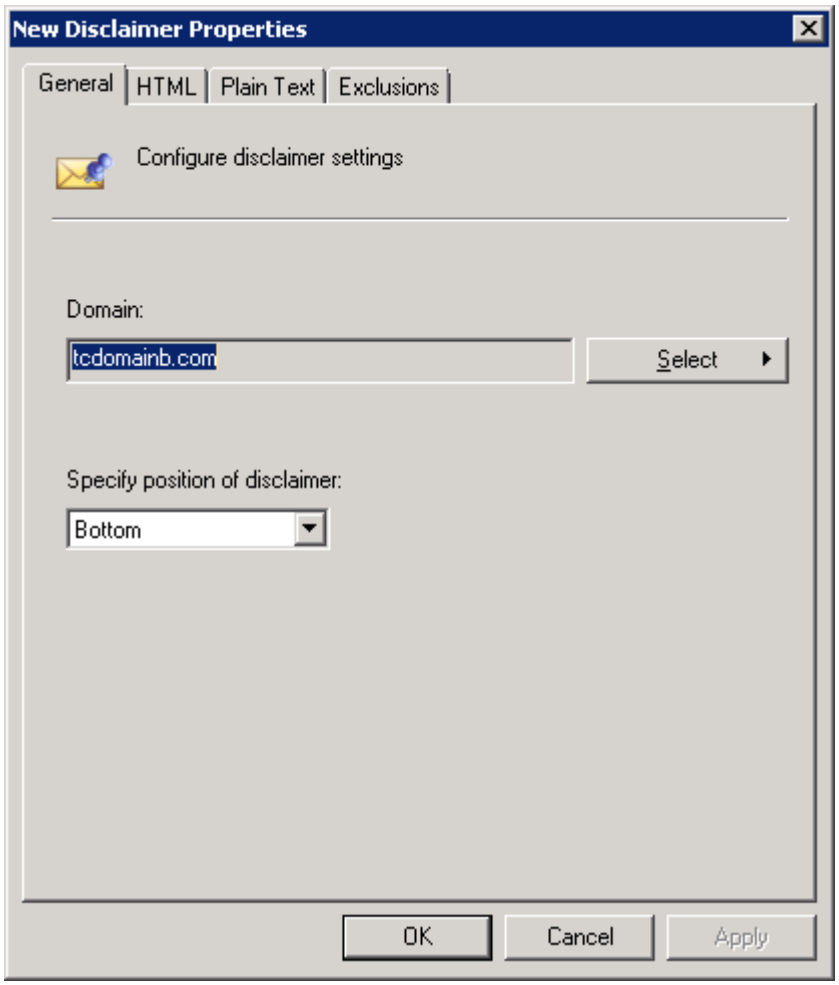
1. Right click **Email Management ► Disclaimers** node and select **New ► Disclaimer**.



Screenshot 57 - Selecting a domain or user disclaimer

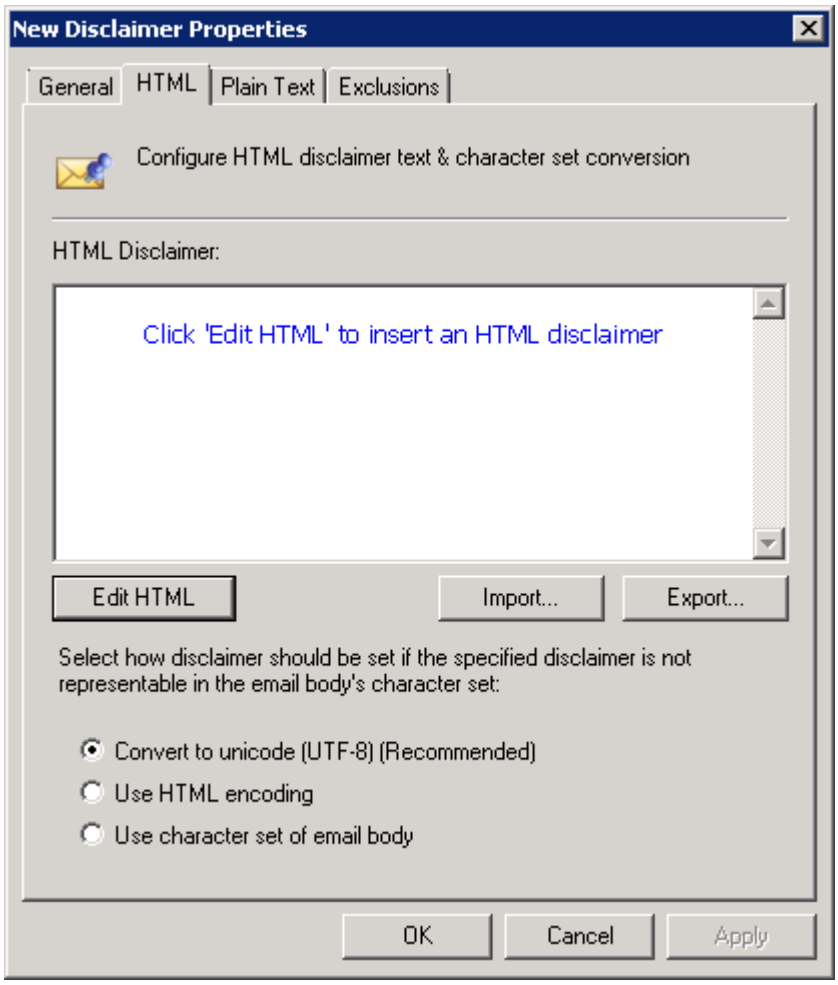
2. Select:

- **Domain** - Choose the domain from the list of configured domains. All emails sent from that domain will have the disclaimer added.
- **User** - Specify a user or a group of users, to whom the disclaimer will be added for outbound emails. If GFI MailEssentials is in Active Directory mode, pick users or groups of users directly from Active Directory; else specify the SMTP email address of the user.



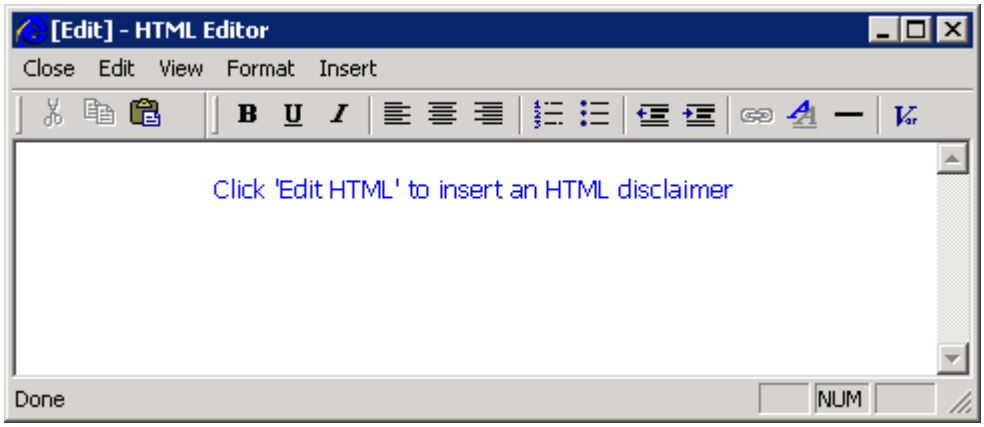
Screenshot 58 - New disclaimer general properties

3. In the **General** tab, click **Select** to change the domain or user. Select **Top** or **Bottom** option to configure if disclaimer should be located at the top or bottom of the email.



Screenshot 59 - HTML disclaimer

4. To add a disclaimer in HTML format, select the HTML tab. Click **Edit HTML** to launch the HTML disclaimer editor and edit the HTML disclaimer text.



Screenshot 60 - The HTML disclaimer editor

5. To add variables in disclaimer, navigate to **Insert ► Variable…**. The variables that can be added are email fields or Active Directory fields. Select the variable to add and click **OK**.

NOTE 1: The recipient display name and email address variables will only be included if the email is sent to a single recipient. If emails are sent to multiple recipients, the variables are replaced with 'recipients'.

NOTE 2: Active Directory fields can only be used when GFI MailEssentials is not installed on the perimeter SMTP server.

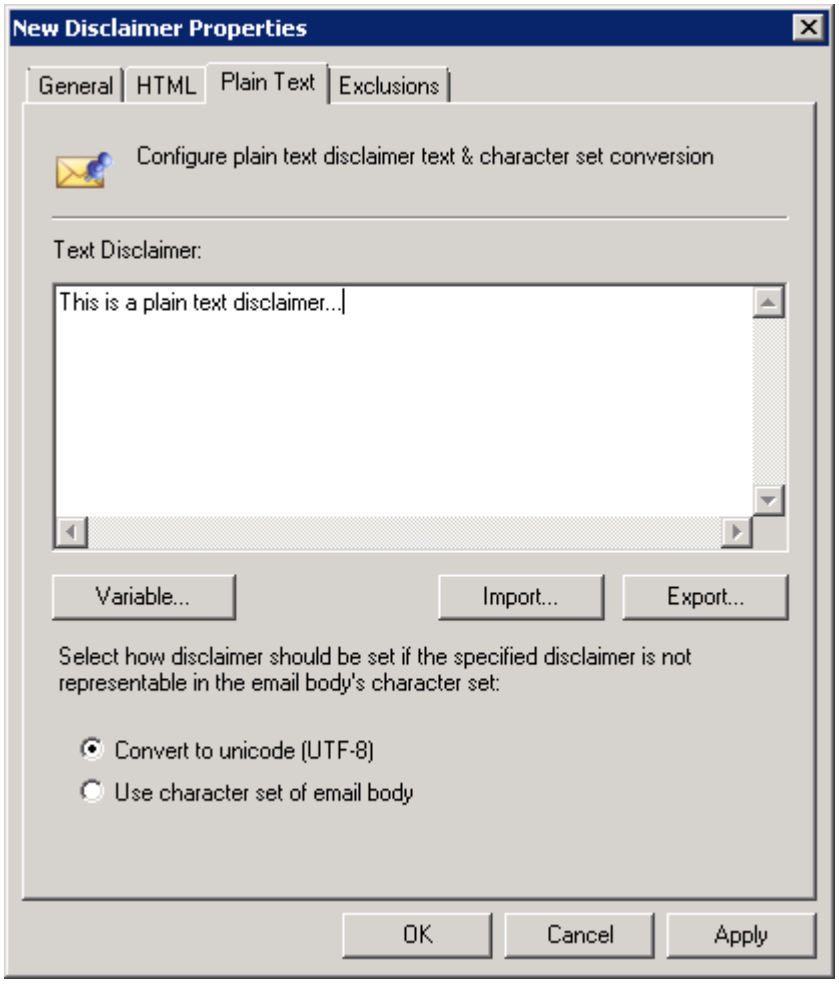
6. Click **Close** when finished editing the HTML disclaimer.

7. Specify the encoding to be used for the HTML disclaimer if the email body's character set is not HTML:

- **Use HTML encoding** - use HTML encoding to define character sets for email body and disclaimer. This option is recommended.
- **Convert to Unicode** - convert both email body and disclaimers to Unicode so that both are properly displayed.
- **Use character set of the email body** - the disclaimer is converted to the email body character set.

  Note: If this option is selected, some of the disclaimer text might not be displayed properly.

8. Import or export an HTML disclaimer in .htm or .html format using the **Import** and **Export** buttons.



Screenshot 61 - Plain text disclaimer

9. A text-based version of your disclaimer can also be included for use in plain text only emails. Select the **Plain Text** tab and insert the text directly into the **Text Disclaimer** field.

10. To add variables in disclaimer click **Variable…**. The variables that can be added are email fields (sender name, recipient email address, etc…) or Active Directory fields (name, title, telephone numbers, etc..). Select the variable to add and click **OK**.

NOTE 1: The recipient display name and email address variables will only be included if the email is sent to a single recipient. If emails are sent to multiple recipients, the variables are replaced with 'recipients'.

NOTE 2: Active Directory fields can only be used when GFI MailEssentials is not installed on the perimeter SMTP server.

11. Specify the encoding to be used for the plain text disclaimer if the email body's character set is not plain text:

- **Convert to Unicode** - convert both email body and disclaimers to Unicode so that both are properly displayed.

» **Use character set of the email body** - the disclaimer is converted to the email body's character set.

Note: If this option is selected, some of the disclaimer text might not be displayed properly.

12. Import or export a plain text disclaimer format using the **Import** and **Export** buttons.

13. From the **Exclusions** tab, specify any senders or recipients for which you do not want to apply this disclaimer. Click **Add** and specify the **User** or **Email Address** to exclude.

NOTE: All recipients must be included in the exclusion list, for a disclaimer not to be added in the email.

14. Click **OK** to save settings.

The newly created disclaimer is displayed in the right pane of the GFI MailEssentials configuration console. To give the new disclaimer a more useful name, right-click on the disclaimer and select **Rename**.

6.1.2 Disabling and enabling disclaimers

By default new disclaimers are automatically enabled. To disable or enable a disclaimer:

1. Right click the disclaimer to disable.

2. Select **Disable** or **Enable** to perform the desired action.

6.2 Auto-replies

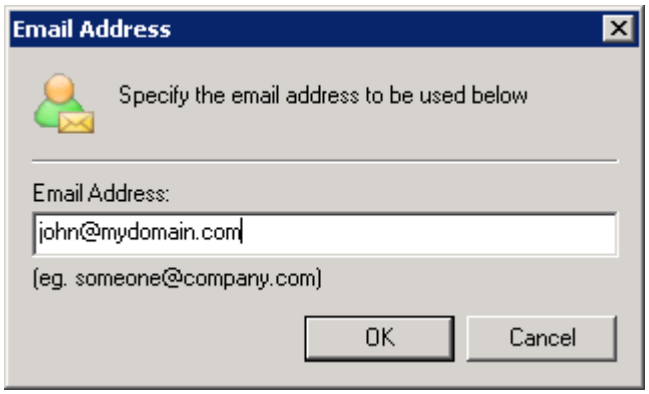
The Auto reply feature enables sending of automated replies to specific inbound emails. A different auto reply for each email address or subject can be specified. You can use variables in an auto reply to personalize an email.

Important notes

1. Do not include any body text beyond 30-40 characters per line and carriage returns. Some older mail servers truncate lines at 30-40 characters.

6.2.1 Configuring auto-replies

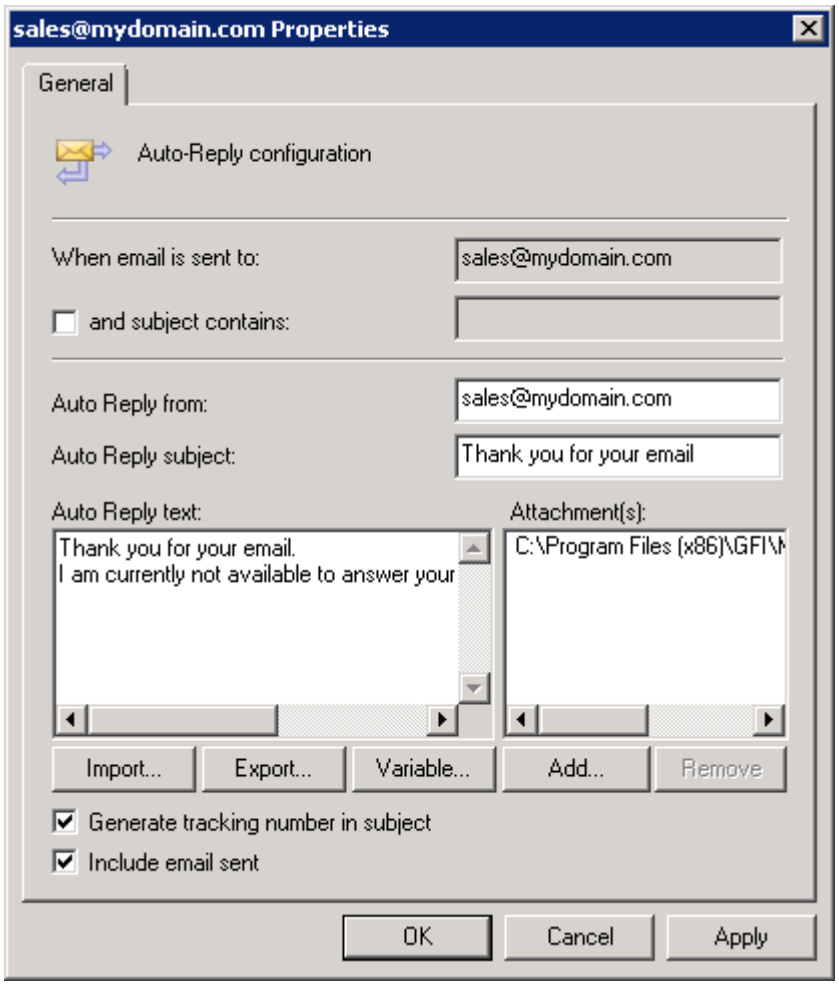
1. Right click **Email management ► Auto-Replies** node and select **New ► Auto-Reply**.



Screenshot 62 - Creating a new auto reply

2. Key in the email address to configure an auto reply and click **OK**.

» **Example** - If 'sales@master-domain.com' is provided, emails sent to this email address will receive an auto reply.



Screenshot 63 - Auto-reply properties

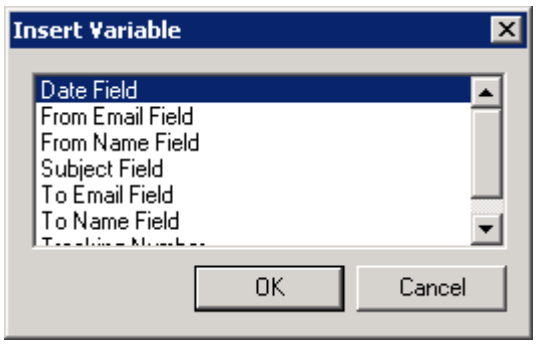
3. Check the **and subject contains** checkbox to enable auto replies for emails containing specific text in the subject field.

4. In the **Auto Reply from:** field, specify an email address in case where an autoreply is required from a different email address other than the email address to which the inbound email was addressed to.

5. In the **Auto Reply subject** field, specify the subject of the auto reply email.

6. In the **Auto Reply text** edit box, specify the text to display in the auto reply email.

NOTE: Import auto reply text from a text file via the **Import...** button.



Screenshot 64 - Variables dialog

7. Click on **Variable...** to personalize auto replies using variables. Select variable field to insert and click **OK**. Available variables are:

- **Date Field** - Inserts the email sent date.
- **From Email Field** - Insert sender email address.
- **From Name Field** - Inserts the display name of the sender.

- **Subject Field** - Inserts email subject.
- **To Email Field** - Inserts the recipient's email address.
- **To Name Field** - Inserts the recipient's display name.
- **Tracking Number** - Inserts tracking number (if generated).

8. Click **Add…** and select any attachments to send with the auto reply email. Remove attachments using the **Remove** button.

9. Select **Include email sent** option to quote the inbound email in auto reply.

10. Select **Generate tracking number in subject** to enable the generation of tracking numbers in the auto replies.

NOTE: This feature enables, for example, customers to reply quoting a tracking number that enables staff to track emails in a more coherent manner.

11. Click **OK** button to finalize settings.

By default, tracking numbers are generated using the following format: `ME_YYMMDD_nnnnnn`

Where:

- **ME -** GFI MailEssentials tag.
- **YYMMDD -** Date in year, month and date format.
- **nnnnnn -** automatically generated tracking number.

6.3 List servers

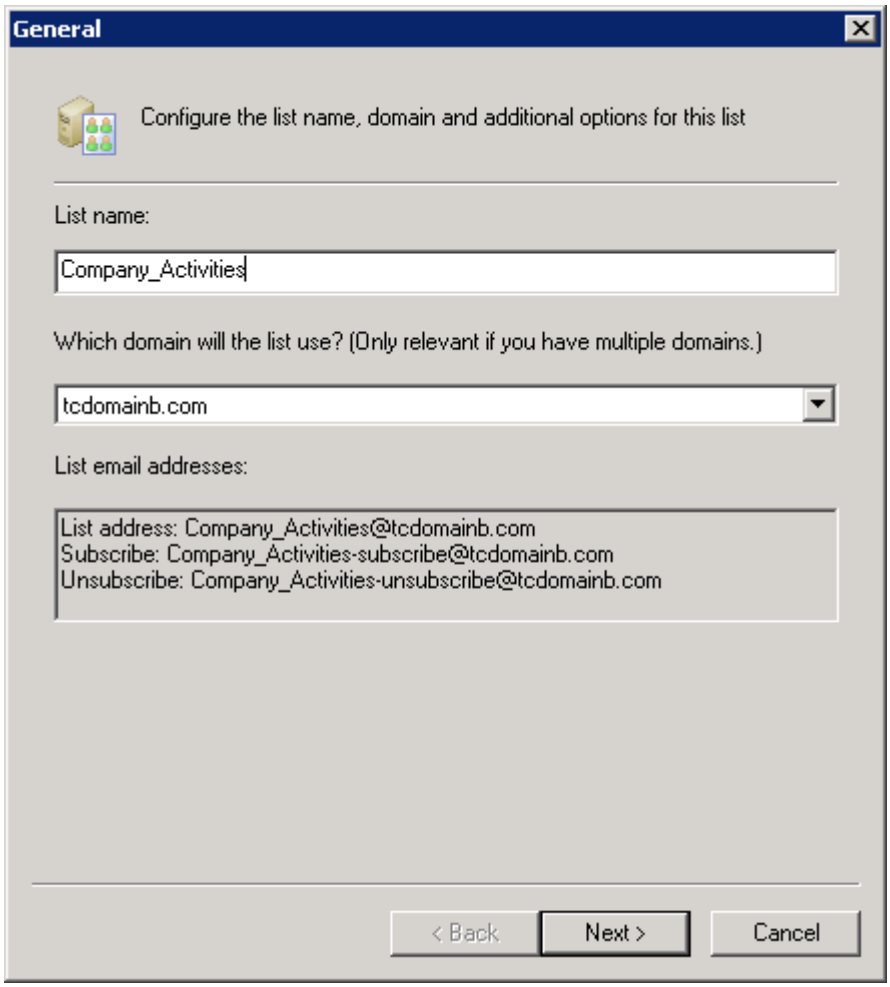
List servers enable the creation of two types of distributions lists:

1. A newsletter subscription list - Used for creating subscription lists for company or product newsletters, to which users can either subscribe or unsubscribe.

2. A discussion list - Enables groups of people to hold discussions via email, with each member of the list receiving the email that a user sends to it.

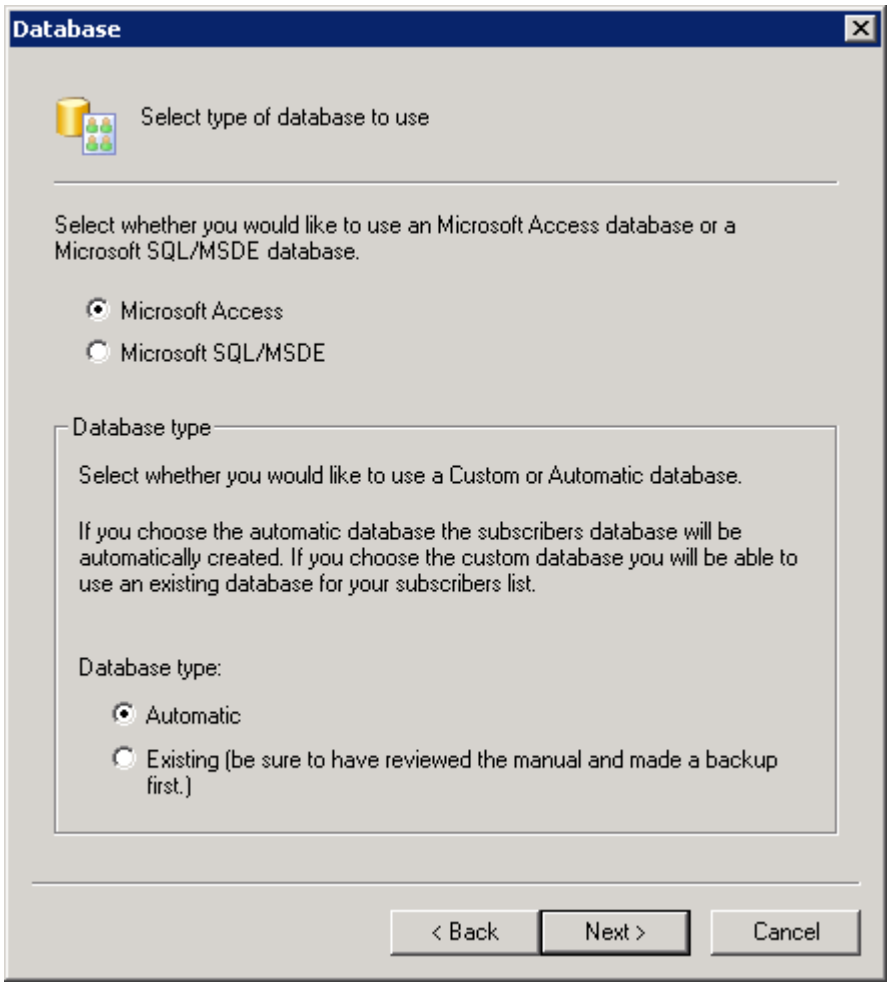
6.3.1 Creating a newsletter or discussion list

1. From the GFI MailEssentials configuration console, right-click **Email Management ► List Server** node and select **New ► Newsletter** or **Discussion List.**



Screenshot 65 - Creating a new newsletter list

2. In the **List name:** field, key in a name for the new list and select a domain for the list (only if you have multiple domains). Click **Next** to continue setup.


Database
Select type of database to use
Select whether you would like to use an Microsoft Access database or a Microsoft SQL/MSDE database.
Microsoft Access
Microsoft SQL/MSDE
Database type
Select whether you would like to use a Custom or Automatic database.
If you choose the automatic database the subscribers database will be automatically created. If you choose the custom database you will be able to use an existing database for your subscribers list.
Database type:
Automatic
Existing (be sure to have reviewed the manual and made a backup first.)
< Back
Next >
Cancel

Screenshot 66 - Specifying database backend

3. Select **Microsoft Access** or **Microsoft SQL Server/MSDE** as database and from the **Database type** group select if GFI MailEssentials should create a new database or connect to an existing database. Click **Next** to continue.

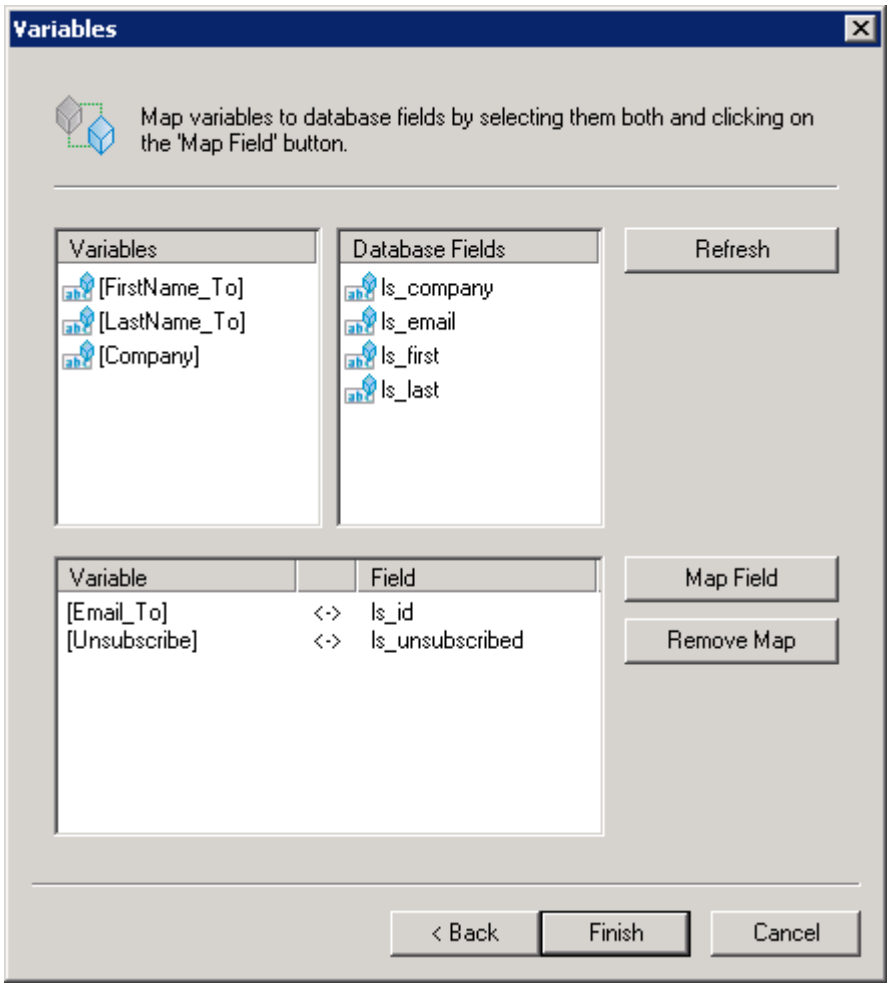
NOTE 1: For small lists of up to 5000 members, you can use Microsoft Access as a backend.

NOTE 2: To create a new database, select the **Automatic** option.

4. Configure the database type selected to store the newsletter/discussion subscribers list. The available options are:

DATABASE TYPE	DATABASE SETTINGS
Microsoft Access with Automatic option	Key in the location where the new database is stored in the File edit box.
Microsoft Access with Existing option	In the File field specify the path to your existing Microsoft Access database that contains the newsletter/discussion subscribers. From the Table drop down list select the table where the subscribers list is stored.
Microsoft SQL Server with Automatic option	Specify SQL server name, logon credentials and database used to store newsletter/discussion subscribers list.
Microsoft SQL with Existing option	Specify SQL server name, logon credentials and select the database and table where subscribers list is stored.

5. For all database types with the **Automatic** option, click **Finish** button to end the wizard, or click **Next** to continue setup.



Screenshot 67 - Mapping custom fields

6. Select a variable from the **Variables** list and the corresponding **Database Field** option and click **Map Field** button to Map the required fields with the custom fields found in the database. Click **Finish** to finalize your configuration. The fields to map are:

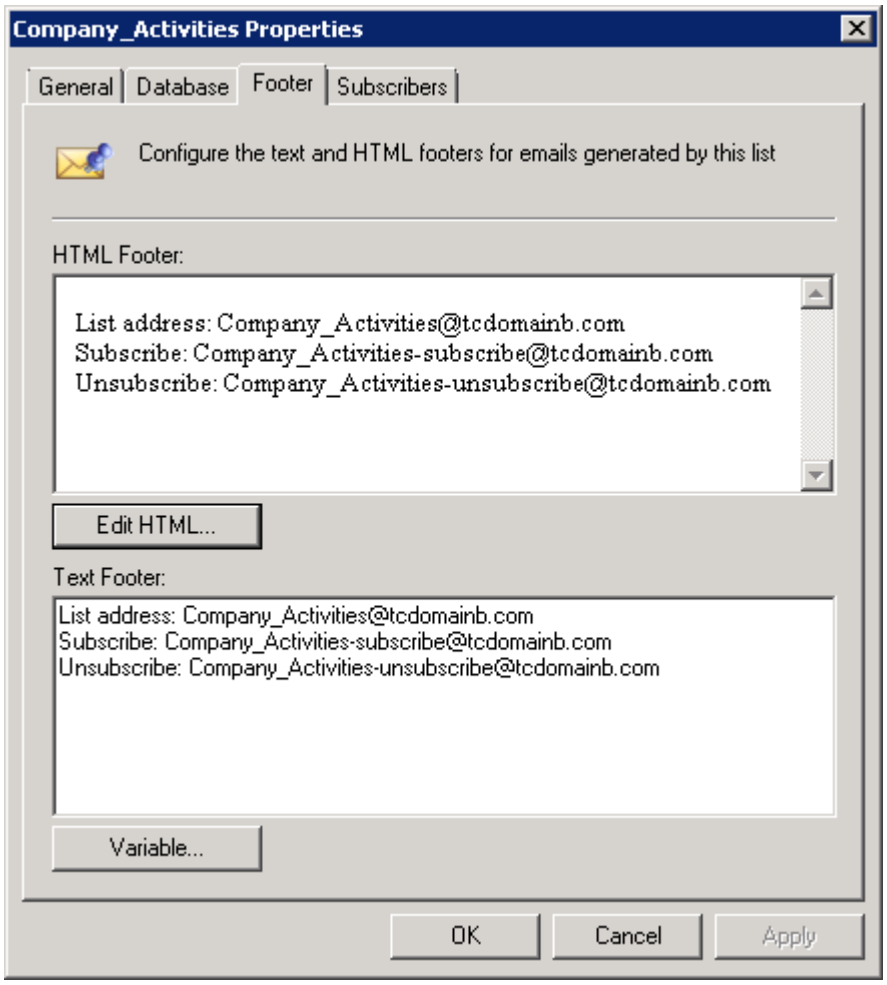
- **[FirstName_To]** - Map to a string field containing the first name of a subscriber.
- **[LastName_To]** - Map to a string field containing the last name of a subscriber.
- **[Company]** - Map to a string field containing the company name of a subscriber.
- **[Email_To]** - Map to a string field containing the email address of a subscriber.
- **[Unsubscribe]** - Map to an integer (or Boolean) value field which is used to define whether the user is subscribed to the list or not.

6.3.2 Configuring advanced newsletter/discussion list properties

- After creating a new list, further options can be configured which enable the customization of elements and behavior of the list.

Creating a custom footer for the list

Configure a custom HTML or text footer. A footer will be added to each email.



Screenshot 68 - Newsletter footer properties

1. Right click the list to add a footer to and select **Properties**.

2. In the **Footer** tab, click **Edit HTML** to create an HTML footer.

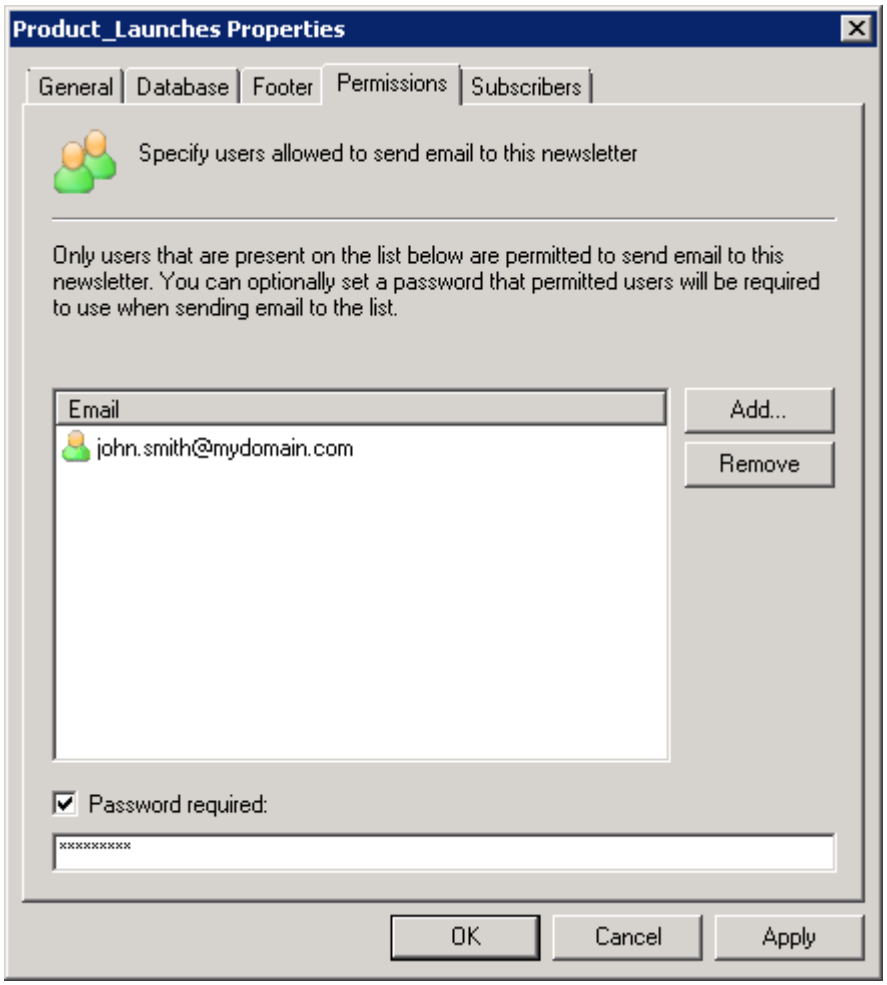
NOTE: Use the footer to communicate how users can subscribe and unsubscribe from the list.

Setting permissions to the list

Specify who can submit an email to the list. If list is not secured, anybody can send an email to the entire list by sending an email to the list address.

NOTE: Permissions are not configurable for discussion lists.

1. Right click the list to set permissions for and select **Properties**.



Screenshot 69 - Setting permissions to the newsletter

2. In the **Permissions** tab, click the **Add** button and specify the users with permissions to submit an email to the list. Email addresses are added to **Email** list.

3. Enable passwords by selecting the **Password required:** checkbox and providing a password. For more information how to use this feature refer to the next section **Securing newsletters with a password**.

Securing newsletters with a password

Set a password which secures access to newsletter/discussion in case someone else makes use of the email client or account details of a permitted user.

NOTE: Discussion lists cannot be secured with passwords.

1. Right click the list to set permissions for and select **Properties**.

2. In the **Permissions** tab, select **Password required:** checkbox and provide a password.

IMPORTANT: Users must authenticate themselves by including the password in the email subject field on sending emails to the newsletter. The password must be specified in the subject field as follows:

[PASSWORD:<*password*>**]** <*The Subject of the email!*>

- **Example:** [PASSWORD:letmepost]Special Offer.

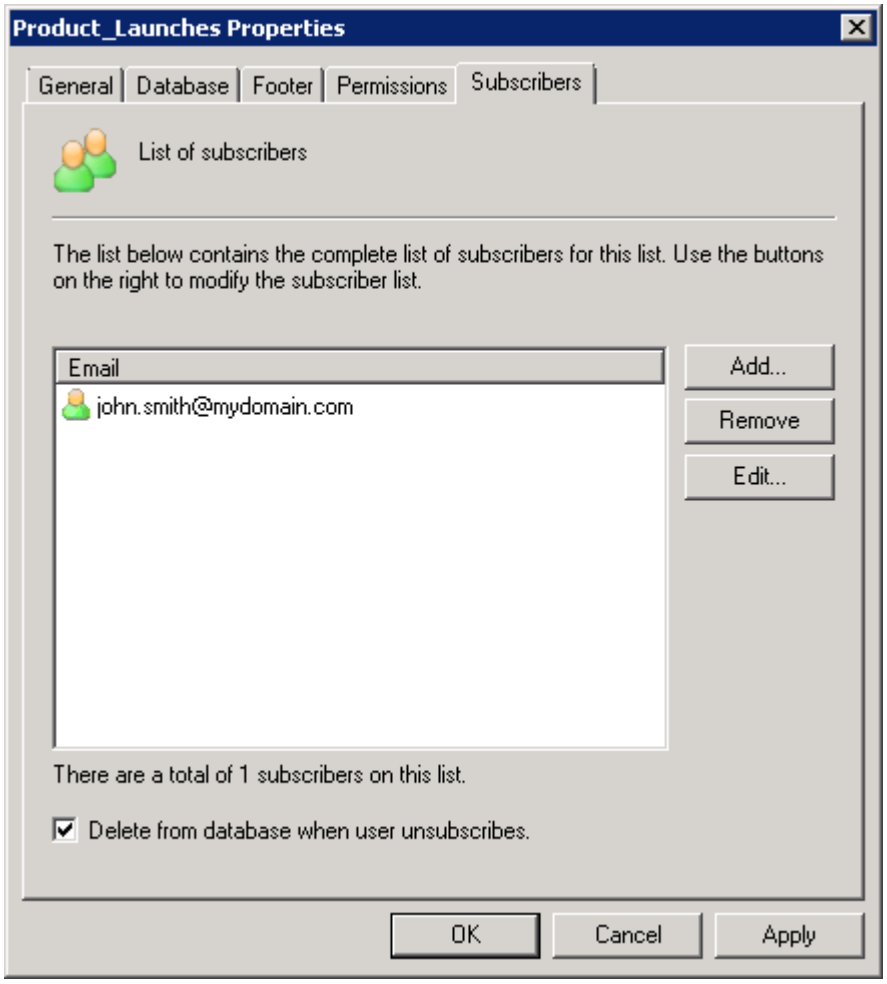
If password is correct, list server will remove the password details from the subject and relay on the email to the Newsletter.

Adding subscribers to the list

Add users to newsletters/ discussions without any action on their behalf.

NOTE: It is highly recommended that users subscribe to the list, by sending an email themselves to the subscribe newsletter/discussion address. Adding users to lists without their explicit permission might generate spam complaints.

1. Right click the list to set permissions for and select **Properties**.



Screenshot 70 - Entering subscribers to the newsletter

2. In the **Subscribers** tab, click **Add** button.

3. Key in **Email Address**, **First name**, **Last name** and **Company** fields and click **OK** button. The new subscriber email address will be added to the **Email** list.

NOTE 1: First name, last name and company fields are optional.

NOTE 2: Select the user and click the **Remove** button to remove subscribers from the list.

NOTE 3: To remove users from the subscription list table when unsubscribing from the list (and not just flag them as unsubscribed) select the **Delete from database when user unsubscribes** checkbox.

6.3.3 Using newsletters/discussions

After creating a newsletter/discussion list, users must subscribe in order to receive it. The actions which users can perform when using newsletters/discussions are:

- Sending a newsletter
- Subscribing to a list
- Completing the subscription process
- Unsubscribing from the list

Using newsletters

- **Subscribing to list** - Ask users to send an email to <newslettername>-subscribe@yourdomain.com

- **Completing the subscription process** - On receiving the request, the list server sends a confirmation email back. Users must confirm their subscription via a reply email to be added as a subscriber.

  NOTE: The confirmation email is a requirement and cannot be turned off.

- **Sending a newsletter/discussion post** - Members with permissions to send email to the list are required to send the email to the newsletter list mailing address:

  <newslettername>@yourdomain.com

- **Unsubscribing from the list** - To unsubscribe from the list, users must send an email to:

  <newslettername>-unsubscribe@yourdomain.com

Tip: To enable users to easily subscribe to newsletters, add a web form asking for name and email address and direct output to:

<newslettername>-subscribe@yourdomain.com

6.3.4 Importing subscribers to the list / database structure

When a new newsletter or discussion list is created, the configuration will create a table called 'listname_subscribers' with the following fields as shown in the table below.

To import data into the list, ensure that the database is populated with the correct data in the correct fields.

FIELD NAME	TYPE	DEFAULT VALUE	FLAGS	DESCRIPTION
Ls_id	Varchar(100)		PK	Subscriber ID
Ls_first	Varchar(250)			First name
Ls_last	Varchar(250)			Last name
Ls_email	Varchar(250)			Email
Ls_unsubscribed	Int	0	NOT NULL	Unsubscribe flag
ls_company	Varchar(250)			Company name

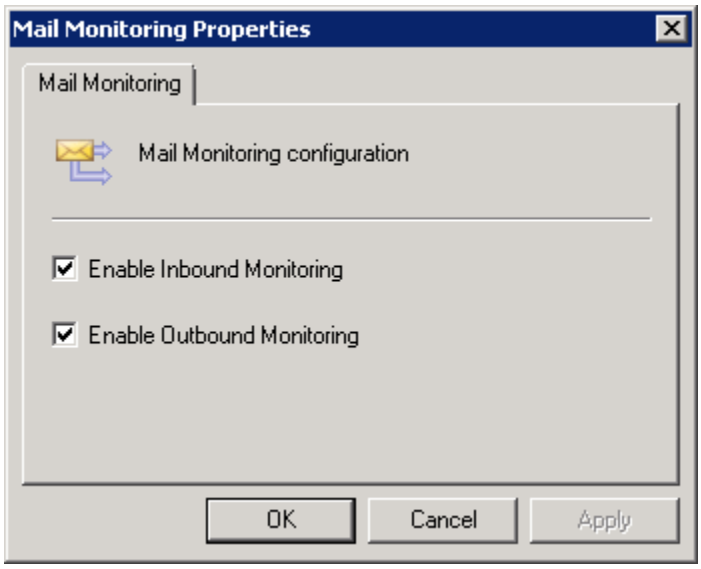
6.4 Email monitoring

Email monitoring enables the sending of copies of emails sent to or from a particular local email address to another email address. This enables the creation of central stores of email communications for particular persons or departments.

This feature can also be used as a replacement for email archiving since emails are automatically sent to Microsoft Exchange Server or Microsoft Outlook store.

6.4.1 Enabling/Disabling email monitoring

1. Right click **Email management ► Mail Monitoring** and select **Properties**.



Screenshot 71 - Enable or disable email monitoring

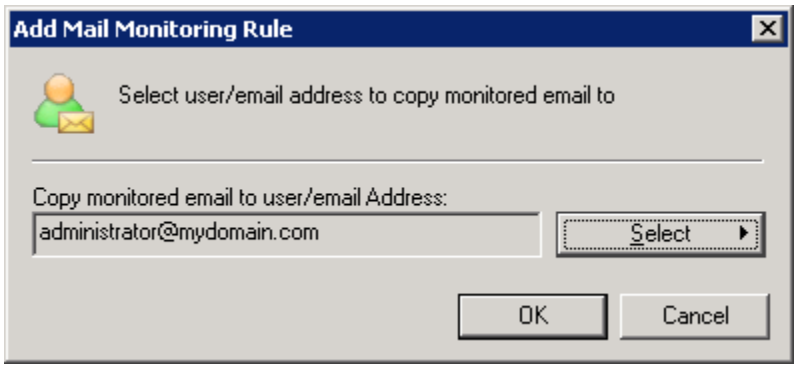
2. Enable/disable all inbound and outbound email monitoring rules by checking/unchecking **Enable Inbound Monitoring** and **Enable Outbound Monitoring** checkboxes.

3. Click **OK** button to save changes.

NOTE: Enable/disable individual email monitoring rules by right click on the email monitoring rule and selecting **Enable/Disable**.

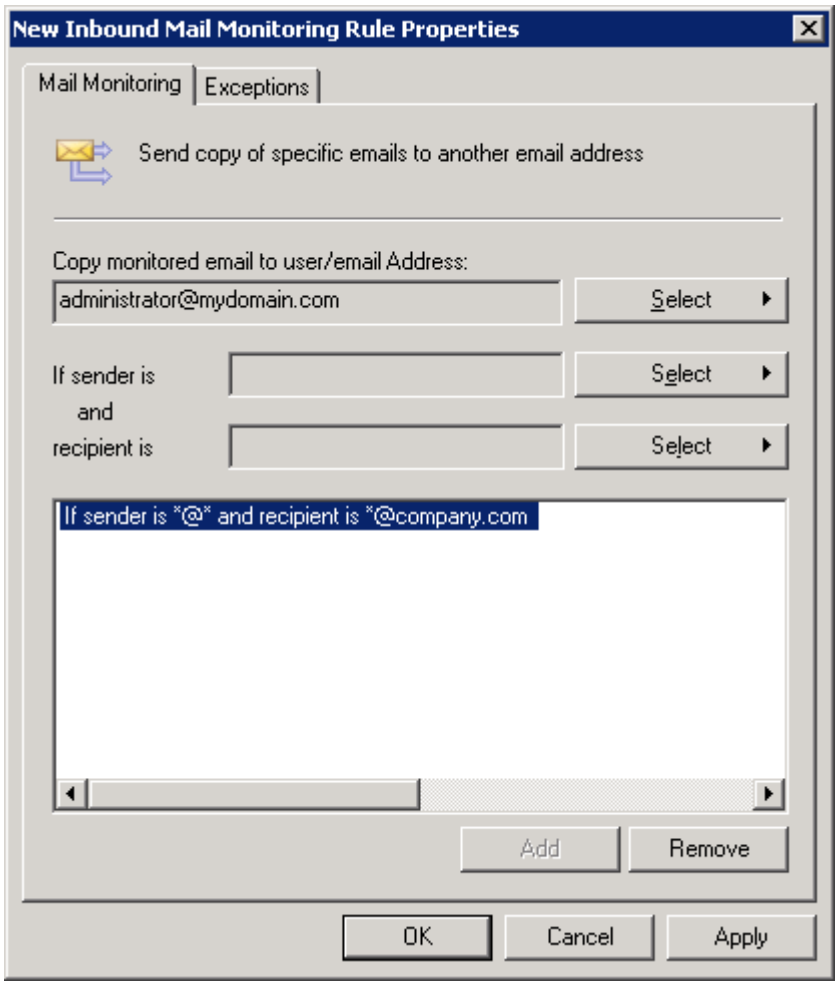
6.4.2 Configure email monitoring

1. Right click **Email management ► Mail Monitoring** node and select **New ► Inbound Mail Monitoring Rule** or **Outbound Mail Monitoring Rule** to monitor inbound or outbound email respectively.



Screenshot 72 - Add Mail Monitoring rule

2. Key in the destination email address/mailbox to copy the emails to. Click **OK** to continue.

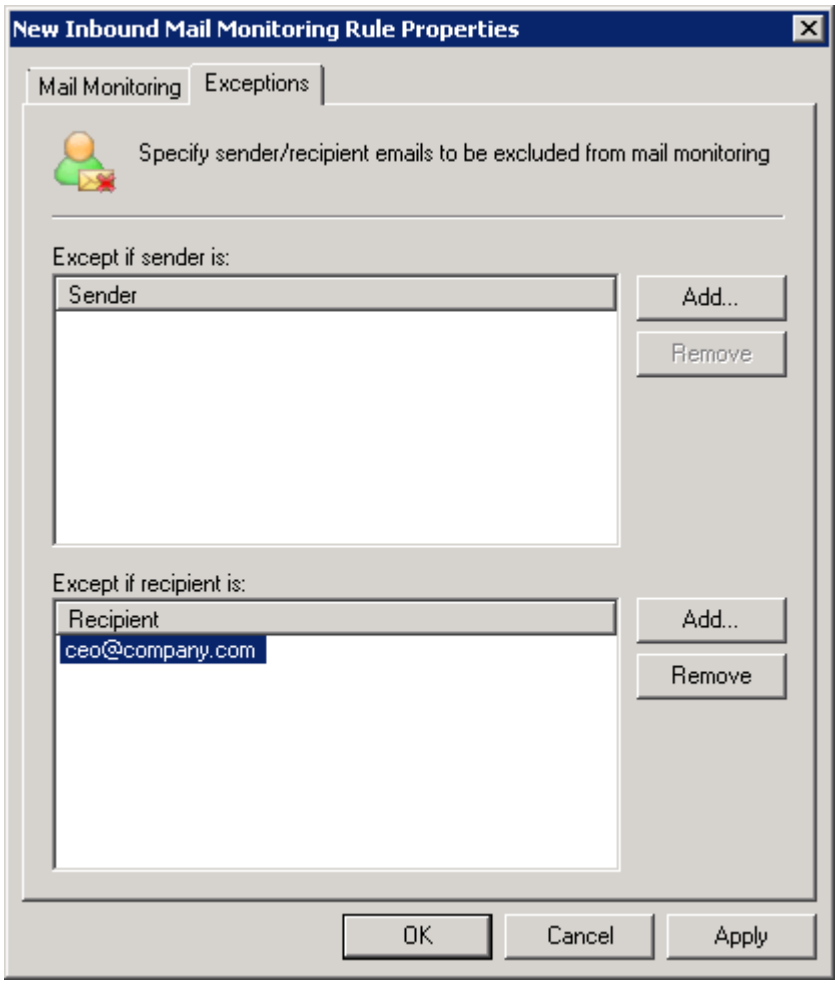


Screenshot 73 - Configuring email monitoring

3. Click sender and recipient **Select** buttons to specify which emails this rule should monitor. Click the **Add** to add filters to the list. Repeat to specify multiple filters. The following conditions can be monitored:

NOTE: To monitor all mail' key in *@*.

- **All email sent by a particular user** - Create outbound rule, specify sender email or select user (if using AD) in the sender field and key in *@* as the recipient's domain.
- **All email sent to a particular user** - Create inbound rule, specify recipient email or select user (if using AD) in the recipient field and specify *@* as the sender's domain.
- **Mail sent by a particular user to an external recipient** - Create an outbound rule, specify sender or select user (if using AD) in the sender field. Key in external recipient email in the recipient field.
- **Mail sent to a particular user by an external sender** - Create an inbound rule and specify external sender email in the sender field. Key in the username or user email address in the recipient field.
- **Mail sent by a particular user to a company or domain** - Create an outbound rule and specify sender or select user (if using AD) in the sender field. Specify the domain of the company in the recipient field by selecting the **domain** via the **recipient** button.
- **Mail sent to a particular user by a company or domain** - Create an inbound rule and specify domain of the company in the sender field. Select **domain** when clicking on the **sender** button and enter username or user email address in the recipient field.



Screenshot 74 - Creating an exception

4. Select the Exceptions tab to add senders or recipients who will be excluded from the new rule. The available options are:

- **Except if sender is** - Excludes the specified sender from the list.
- **Except if recipient is** - Excludes the specified recipient from the list.

NOTE 1: When specifying exceptions for inbound monitoring rules, the **Sender** list contains non-local email addresses and the **Recipient** list addresses are all local. When specifying exceptions for an outbound monitoring rule, the **Sender** list contains local email addresses, whilst the **Recipient** list contains only non-local email addresses.

NOTE 2: Both exception lists apply and all senders listed in the sender exception list and all recipients listed in the recipient list will not be monitored.

5. Click **OK** to finalize settings.

NOTE: The new email monitoring rule can be renamed by clicking on the rule and pressing the F2 key.

7 Customizing GFI MailEssentials setup

7.1 Inbound email domains

Inbound Email Domains enable GFI MailEssentials to distinguish between inbound and outbound email and therefore to identify which emails should be scanned for spam. During installation, inbound email domains are imported from the IIS SMTP service.

In some cases however local email routing in IIS might be required to be configured differently:

» **Example:** To add domains which are local for email routing purposes but are not local for your mail server.

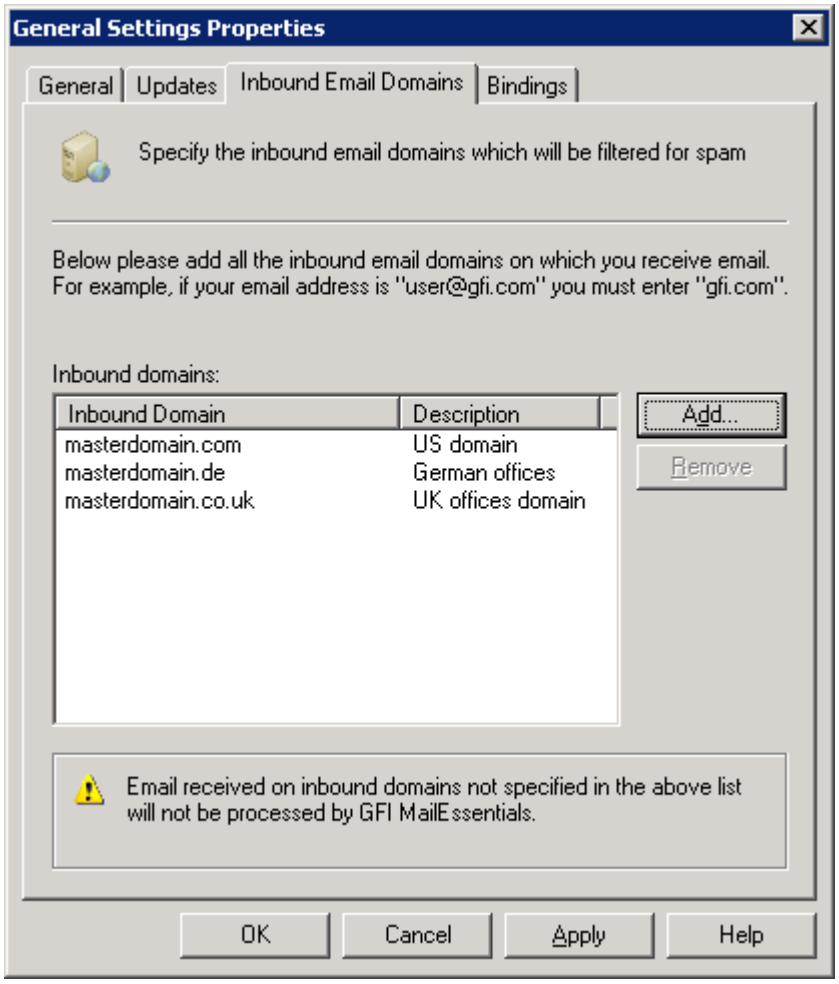
The instructions in this section show how to add or remove inbound email domains after installation.

Important notes

Any domain on which you receive email that is not listed in the inbound domains setup is not protected against spam by GFI MailEssentials

7.1.1 Adding and removing inbound domains

1. Right click **General ► General Settings**, select **Properties** and click on **Inbound Email Domains** tab.



Screenshot 75 - Adding an inbound email domain

2. Click **Add...** button and key in domain details to add new inbound email domains. To remove domains, select the domain to remove and click **Remove**.

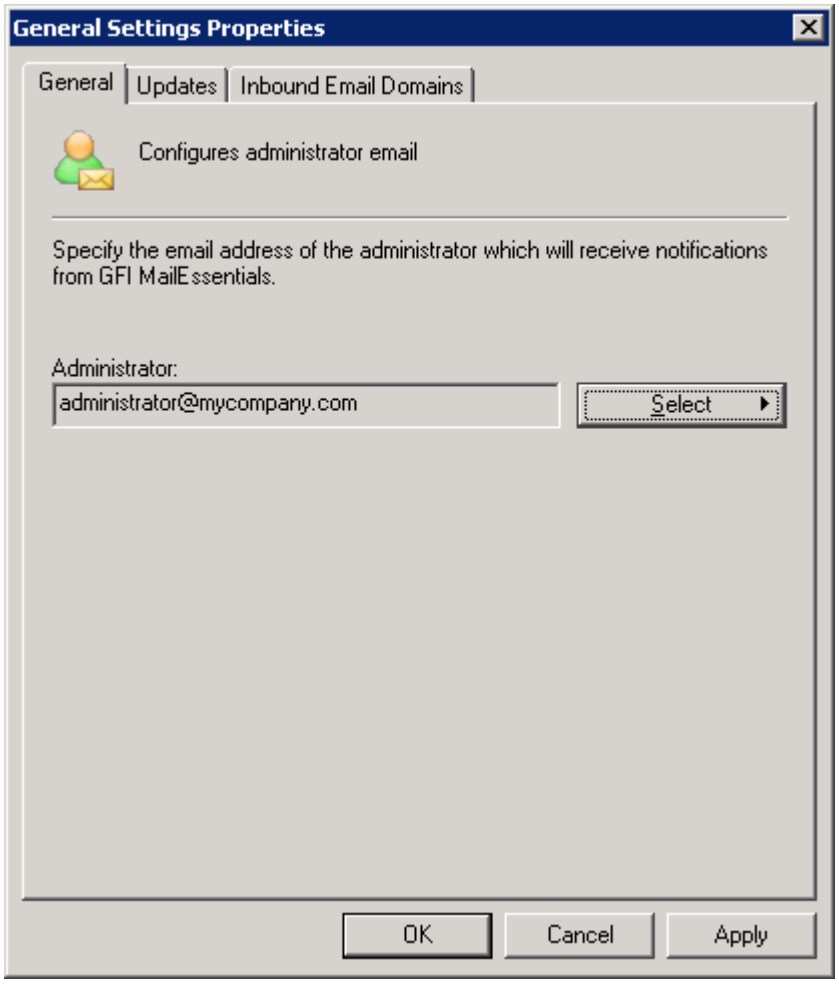
3. Click **OK** to finalize settings.

7.2 Administrator email address

GFI MailEssentials sends various email notifications to the administrator. These include warnings, spam digests and update notifications.

To configure the administrator email address:

1. From the GFI MailEssentials Configuration right-click **GFI MailEssentials ► General ► General Settings** and select **Properties**.



Screenshot 76 - Administrator email address

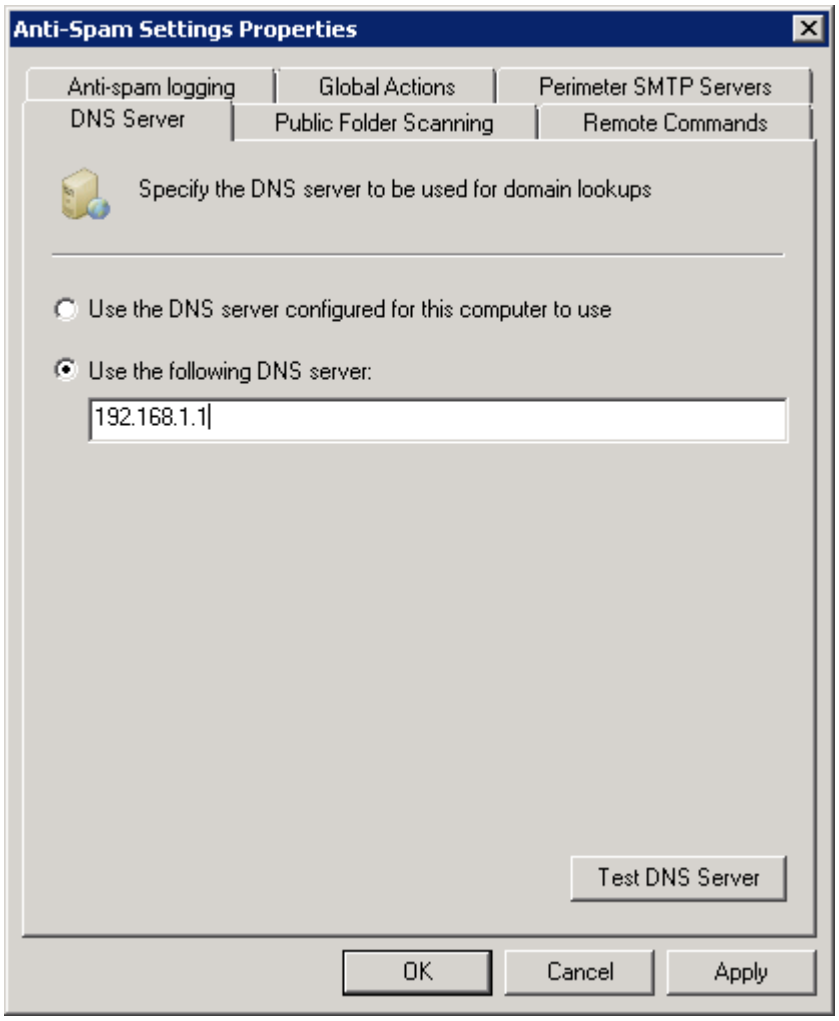
2. From the General tab click **Select** and specify a user or an email address.

3. Click **OK** to finalize settings.

7.3 DNS server settings

DNS Server settings are very important in GFI MailEssentials since IP DNS Blocklist and URI DNS Blocklist perform domain lookups when filtering spam. Other anti-spam filters also use DNS to filter spam (e.g. SpamRazer).

1. From the GFI MailEssentials Configuration right-click **GFI MailEssentials ► Anti-Spam ► Anti-Spam Settings** and select **Properties**.



Screenshot 77 - DNS server settings

2. From the DNS Server tab select:

- **Use the DNS server configured for this computer to use** - Select this option to use the same DNS server that is used by the operating system where GFI MailEssentials is installed.
- **Use the following DNS server** - Select this option to specify a DNS server that is different than the one used by the local machine IP address.

3. Click **Test DNS Server** to test connection with the specified DNS server. If test is unsuccessful, specify another DNS server.

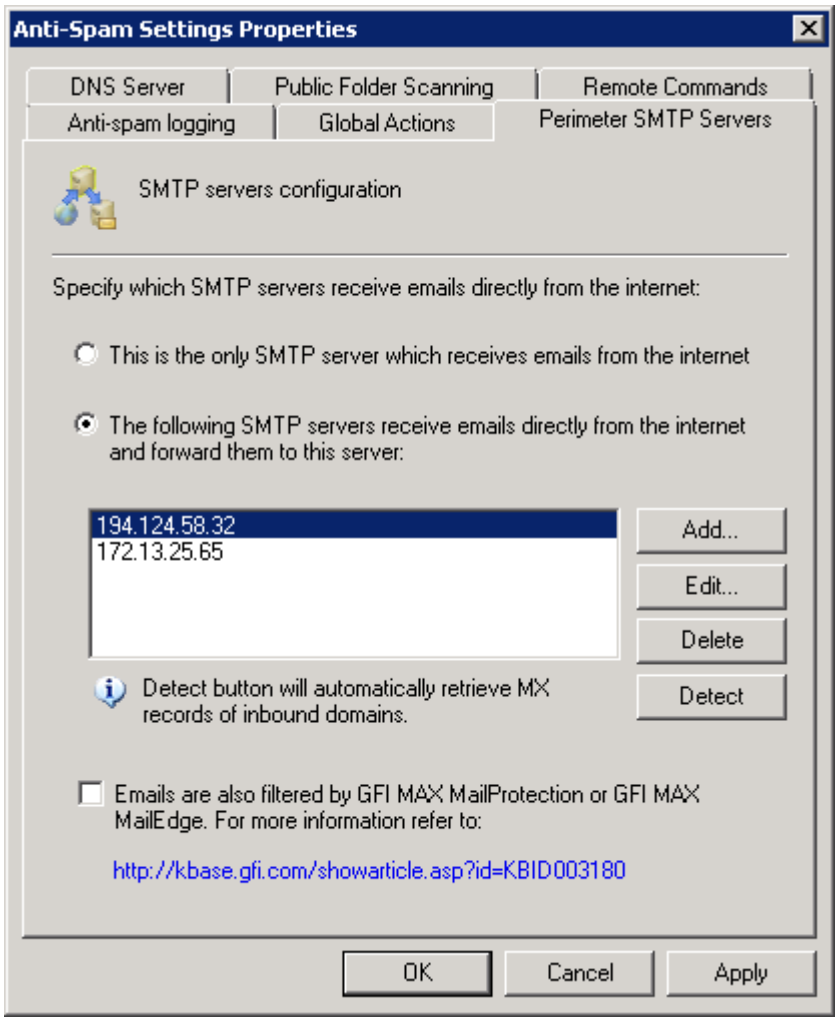
4. Click **OK** to finalize settings.

7.4 SMTP Server settings

SMTP servers that relay emails to the GFI MailEssentials server must be specified for various anti-spam filtering modules, such as IP DNS Blocklist and Greylist.

To specify the perimeter SMTP servers:

1. From the GFI MailEssentials Configuration right-click **GFI MailEssentials ► Anti-Spam ► Anti-Spam Settings** and select **Properties**.


Anti-Spam Settings Properties
DNS Server
Public Folder Scanning
Remote Commands
Anti-spam logging
Global Actions
Perimeter SMTP Servers
SMTP servers configuration
Specify which SMTP servers receive emails directly from the internet:
This is the only SMTP server which receives emails from the internet
The following SMTP servers receive emails directly from the internet and forward them to this server:
194.124.58.32
172.13.25.65
Add...
Edit...
Delete
Detect
Detect button will automatically retrieve MX records of inbound domains.
Emails are also filtered by GFI MAX MailProtection or GFI MAX MailEdge. For more information refer to:
http://kbase.gfi.com/showarticle.asp?id=KBID003180
OK
Cancel
Apply

Screenshot 78 - Perimeter SMTP Server settings

2. From the Perimeter SMTP Servers tab select:

- **This is the only SMTP server which receives emails from the internet** when GFI MailEssentials is installed on the only SMTP server that receives external emails directly from the internet.
- **The following SMTP servers receive emails directly from the internet and forward them to this server** when emails are relayed to the GFI MailEssentials server from other SMTP servers. Click **Detect** to instruct GFI MailEssentials to automatically detect SMTP servers by retrieving MX records of inbound domains. Click **Add** to manually add the IPs of any other SMTP servers that relay emails to the GFI MailEssentials server and that were not automatically discovered.

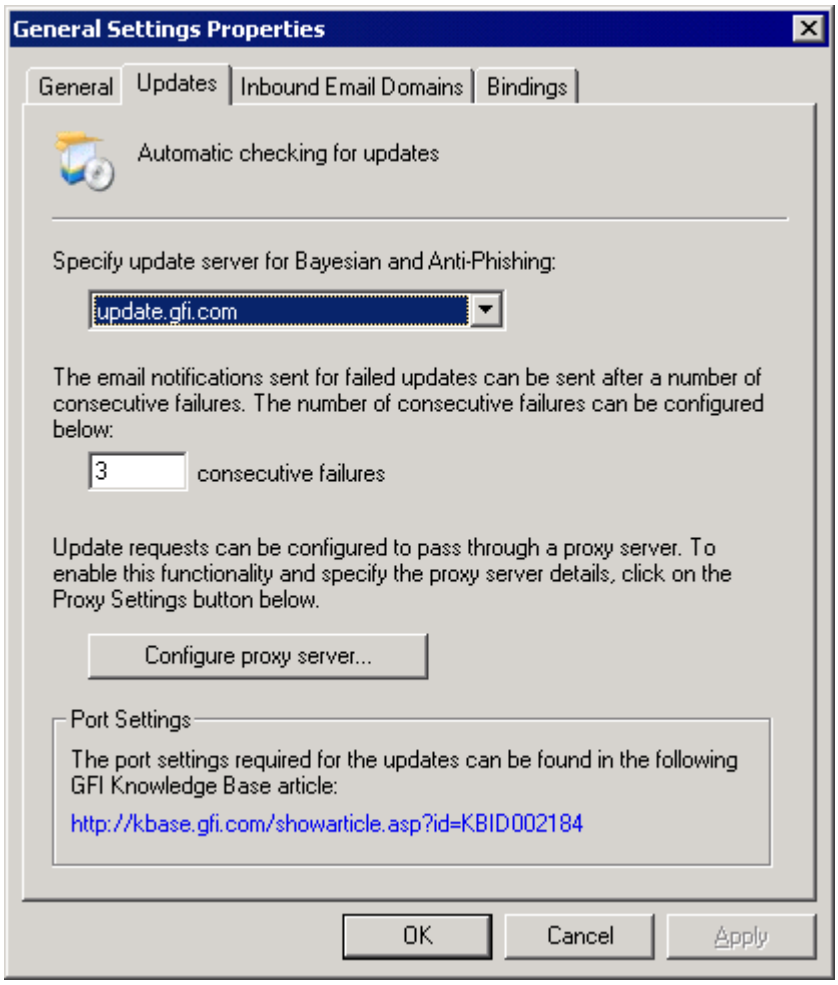
  NOTE: When manually adding IPs of perimeter SMTP servers, you can also add a range of IP addresses using the CIDR notation.
- **Emails are also filtered by GFI MAX MailProtection or GFI MAX MailEdge** when using hosted email security products GFI MAX MailProtection or GFI MAX MailEdge. For more information refer to:

  http://kbase.gfi.com/showarticle.asp?id=KBID003180

3. Click **OK** to finalize settings.

7.5 Automatic updates

GFI MailEssentials can be configured to automatically check for and download updates.


General Settings Properties
General
Updates
Inbound Email Domains
Bindings
Automatic checking for updates
Specify update server for Bayesian and Anti-Phishing:
update.gfi.com
The email notifications sent for failed updates can be sent after a number of consecutive failures. The number of consecutive failures can be configured below:
3
consecutive failures
Update requests can be configured to pass through a proxy server. To enable this functionality and specify the proxy server details, click on the Proxy Settings button below.
Configure proxy server...
Port Settings
The port settings required for the updates can be found in the following GFI Knowledge Base article:
http://kbase.gfi.com/showarticle.asp?id=KBID002184
OK
Cancel
Apply

Screenshot 79 - Configuring automatic updates

1. To configure automatic updates right click **General ► General Settings** node, select **Properties** and click on **Updates** tab.

   - » Specify the updates server used to check for and download any Bayesian spam filter updates and Anti-Phishing updates.
   - » Specify the number of consecutive update failures before sending an email notification.
   - » To download updates using a proxy server click **Configure proxy server…**. In the Proxy Settings dialog specify the settings of the proxy server.

2. Click **OK** to finalize your configuration.

8 Miscellaneous

This section describes all the other features that fall outside the initial configuration, daily management and customization of GFI MailEssentials.

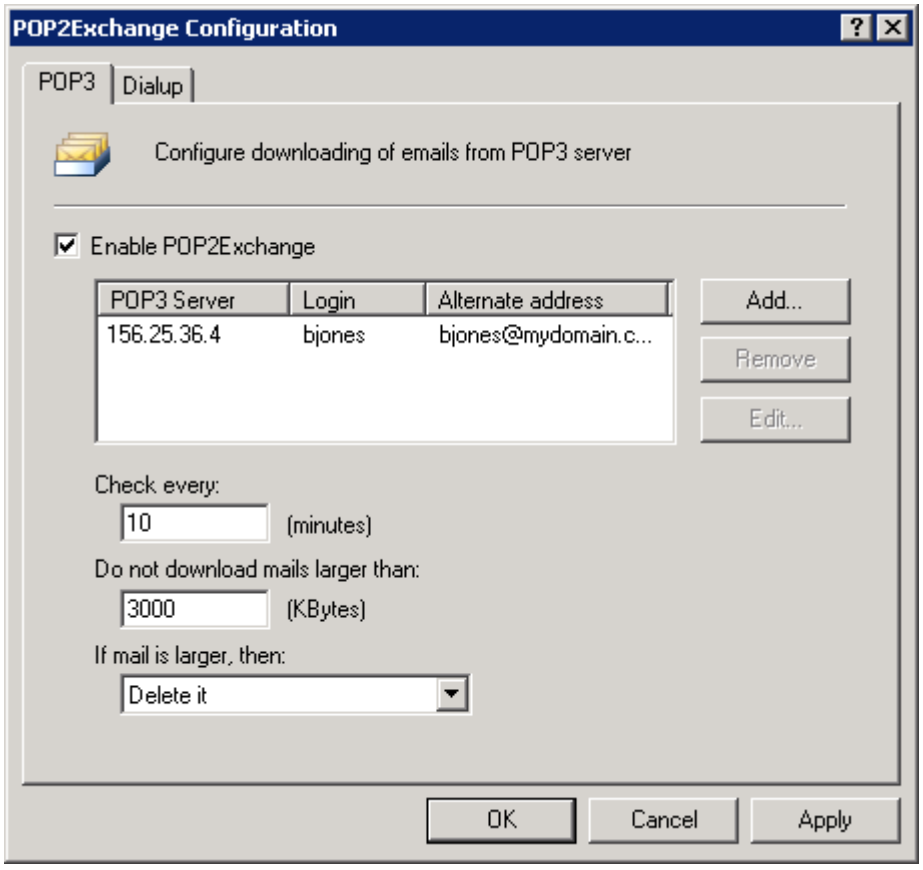
8.1 Setting up POP3 and dialup downloading

Post office protocol (POP3 - RFC 1225) is a client/server protocol for storing email so that clients can connect to the POP3 server at any time and read the email. A mail client will make a TCP/IP connection with the server and by exchanging a series of commands, enable users to read the email. All ISPs support POP3.

The recommendation for GFI MailEssentials is to, if possible, avoid using POP3 and to use SMTP since POP3 is designed for email clients and not for mail servers. Notwithstanding this fact, and to cater for situations where a static IP address used with SMTP is not available, GFI MailEssentials can use POP3 to retrieve email.

8.1.1 Configuring the POP3 downloader

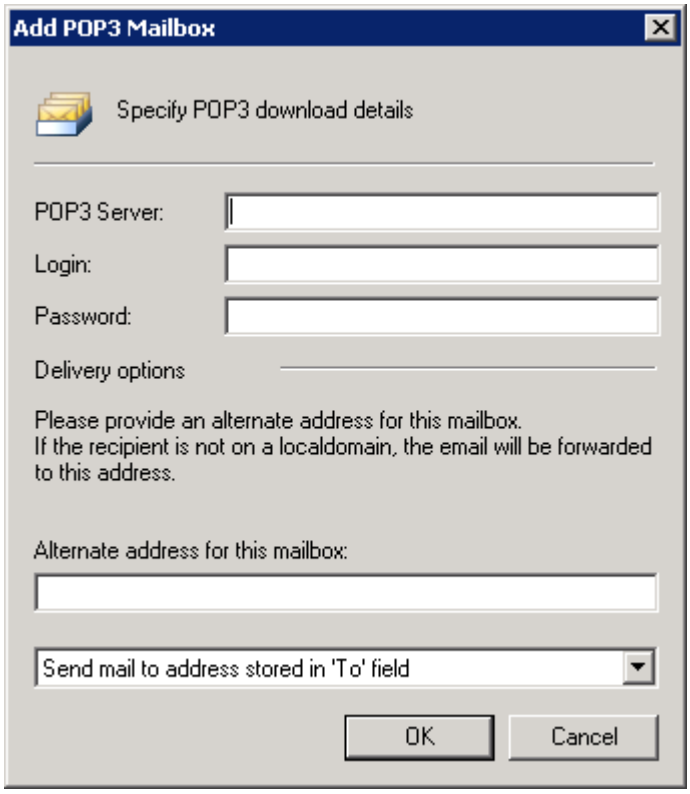
1. Select **POP2Exchange** node and double click **General**.



Screenshot 80 - The GFI MailEssentials pop3 downloader

2. In the **POP3** tab, select **Enable POP2Exchange** checkbox to enable POP3 downloader.

3. Click **Add** to add a POP3 mailbox from which to download email.


Add POP3 Mailbox
Specify POP3 download details
POP3 Server:
Login:
Password:
Delivery options
Please provide an alternate address for this mailbox.
If the recipient is not on a localdomain, the email will be forwarded to this address.
Alternate address for this mailbox:
Send mail to address stored in 'To' field
OK
Cancel

Screenshot 81 - Adding a POP3 mailbox

4. Key in the POP3 server details, mailbox login name and password of the mailbox. Choose between:

- **Send mail to address stored in 'To' field -** GFI MailEssentials will analyze the email header and route the email accordingly. If email analyzing fails, email is sent to the email address specified in the alternate address field.
- **Send mail to alternate address:** All email from this mailbox is forwarded to one email address. Enter full SMTP address in the 'Email address' field.
  - **Example:** john@company.com

5. Provide the alternate address and click **OK**.

NOTE 1: When specifying the destination email address (the address where GFI MailEssentials will forward the email to), ensure that you have set up a corresponding SMTP address on your mail server.

NOTE 2: Multiple POP3 mailboxes can be configured.

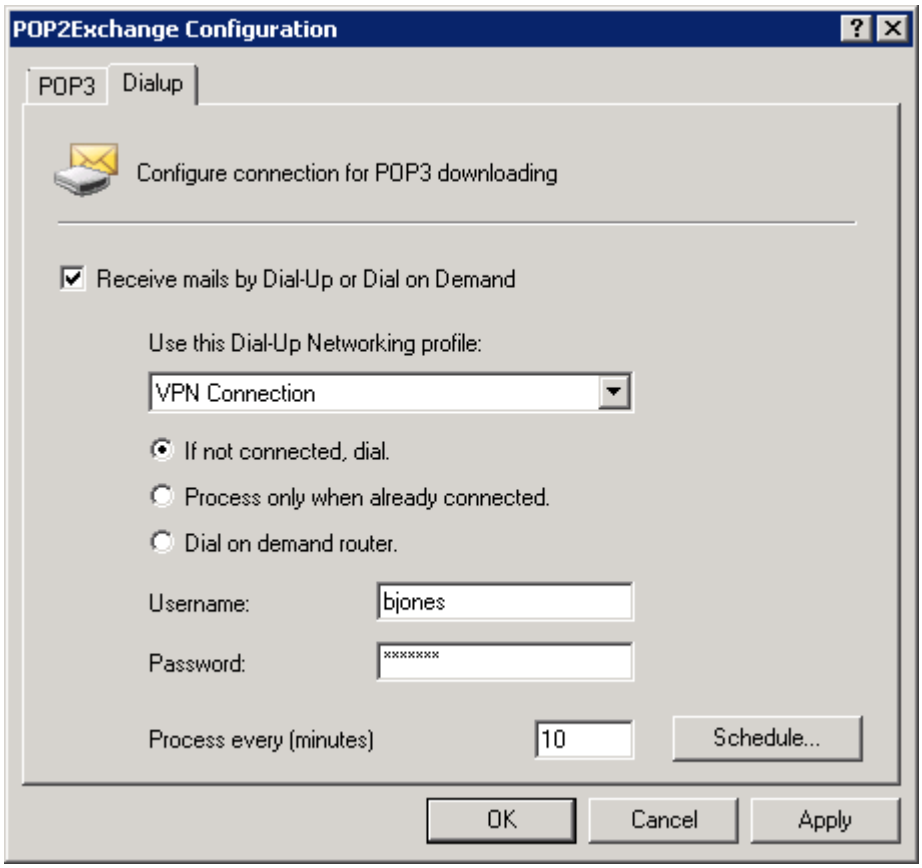
6. In the POP2Exchange configuration dialog, configure other available options:

- **Check every (minutes):** Specify the download interval.
- **Do not download mail larger than (Kbytes):** Specify a maximum download size. If email exceeds this size, it will not be downloaded.
- **If mail is larger, then:** Choose to delete email larger than the maximum allowed size, or send a message to the postmaster.

8.1.2 Configure dial up connection options

1. Select **POP2Exchange** node and double click **General** item.

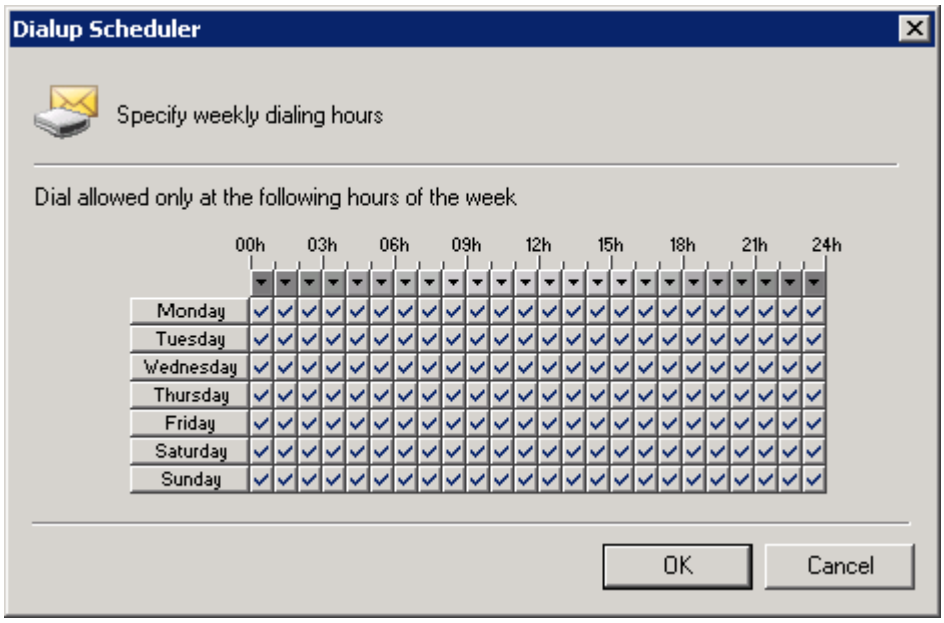
2. From the **Dialup** tab select **Receive mails by Dial-Up or Dial on Demand** checkbox to enable dialup.



Screenshot 82 - Dial-up options

3. Select a dial-up networking profile and configure a login name and password. The following options are available:

- **Use this Dial-Up Networking profile:** Choose the Dial-up Networking profile to use.
- **If not connected dial:** GFI MailEssentials will only dial-up if there is no connection.
- **Username:** Enter the username used to logon to your ISP.
- **Password:** Enter the password used to logon to your ISP.
- **Process only when already connected:** GFI MailEssentials will only process email if a connection already exists.
- **Dial on demand router:** In case of an internet connection that is automatically established (such as a dial on demand router) select this option. GFI MailEssentials will pick up email at the specified interval without triggering a dial-up connection.
- **Process every (minutes):** Enter the interval at which GFI MailEssentials must either dial-up or check if a connection already exists (depends on whether you set GFI MailEssentials to dial-up or to only process email when already connected).



Screenshot 83 - Configuring when GFI MailEssentials should pick up email

4. Click on **Schedule** and specify the hours when GFI MailEssentials should dial-up to pick up email. A check mark indicates that GFI MailEssentials will dial out. A cross indicates that GFI MailEssentials will not dial out at this hour.

5. Click **OK** to finalize your configuration.

8.2 Synchronizing configuration data

When GFI MailEssentials is installed on multiple servers, it is important to keep the anti-spam and configuration data synchronized between servers.

GFI MailEssentials automates this process through two features that keep multiple GFI MailEssentials installations synchronized:

- **Anti-spam synchronization agent:** This service takes care of keeping anti-spam settings synchronized between GFI MailEssentials installations using the Microsoft BITS service.
- **GFI MailEssentials Configuration Export/Import Tool**: This application enables the export and import of all GFI MailEssentials configuration settings and enables the configuration of a new GFI MailEssentials installation with the same exact settings of an already working GFI MailEssentials installation.

8.2.1 Anti-spam synchronization agent

The Anti-Spam Synchronization Agent works as follows:

1. A server machine hosting GFI MailEssentials is configured as the master server.

2. The other server machines, where GFI MailEssentials is installed, are configured as slave servers.

3. The slave servers upload an archive file, containing the anti-spam settings, to an IIS virtual folder hosted on the master server via the BITS service.

4. When the master server has collected all the slave servers anti-spam data, the data is extracted from the individual archives and merged into a new up to date anti-spam settings archive file.

5. The slave servers download this updated anti-spam settings archive file and take care of extracting it and updating the local GFI MailEssentials installation to make use of the new settings.

NOTE 1: The servers that collaborate in the synchronization of anti-spam settings must all have the same version of GFI MailEssentials installed.

NOTE 2: The files uploaded and downloaded by the anti-spam synchronization agent are compressed to limit the traffic on the network.

8.2.2 Step 1: Configuring the Synchronization Agent virtual directory on the master server

Important notes

1. Only one server can be configured as master server at any one time.

2. To configure a server as a master server, it must meet one of the following system specifications:

- Microsoft Windows Server 2008 with SP1 or later and IIS 7.0, with BITS server extensions installed. (Further information how to install the BITS server extension is provided below)
- Microsoft Windows Server 2003 with SP1 or later and IIS 6.0 with BITS server extension installed. (Further information on how to install the BITS server extension is provided below)

3. Install the Microsoft BITS server extensions:

- Windows Server 2003 refer to:

  http://technet.microsoft.com/en-us/library/cc740133(WS.10).aspx

- Windows Server 2008 refer to:

  http://technet.microsoft.com/en-us/library/cc753301.aspx

4. An IIS virtual directory should be created on the master server only.

Synchronization Agent virtual directory configuration

In Internet Information Services (IIS) Manager, configure a shared virtual directory on the default website of the master server as described below.

IIS 7.0

a. Load the **Internet Information Services (IIS) Manager** console, right click on the website of your choice and select **Add Virtual Directory**.

b. In the **Add Virtual Directory** dialog, key in **MESynchAgent** as an alias for the virtual directory.

c. Specify a path where to store the contents for this virtual directory and click **OK** to add the virtual directory.

NOTE: Keep note of the configured path for reference.

d. Select **MESynchAgent** virtual directory and from the Features View, double click **SSL Settings**.

e. Disable the **Require SSL** checkbox and click **Apply**.

f. Return to the Features View of the newly added virtual directory and double click **Authentication**.

g. Ensure that only **Basic Authentication** is enabled, while the other options are disabled.

h. Right click **Basic Authentication** and click **Edit…** to specify the **Default Domain** and **Realm** of the username and password used for authentication by the slave machines. Click **OK** and **Apply**.

i. Return to the Features View of **MESynchAgent** virtual directory and double click **BITS Uploads**.

j. Select **Allow clients to upload files** and select **Use default settings from parent**. Click **Apply**.

IIS 6.0

a. From the **Administrative Tools** group, load the **Internet Information Services (IIS) Manager** console, right click on the website of your choice and select **New ► Virtual Directory**.

b. In the **Virtual Directory Creation Wizard** key in **MESynchAgent** as an alias for the virtual directory and click **Next**.

c. Specify a path where to store the contents for this virtual directory and click **Next**.

NOTE: Keep note of the configured path for reference.

d. Select **Read** and **Write** checkboxes and uncheck all other checkboxes. Click **Next** and click **Finish**.

e. Right click **MESynchAgent** virtual directory and select **Properties**.

f. Select **Directory Security** tab and in the **Authentication and access control** group click **Edit**.

g. In **Authenticated access** group check **Basic Authentication** checkbox and specify **Default domain** and **Realm** of the username and password used for authentication by the slave machines.

NOTE: Ensure that all other checkboxes are unchecked.

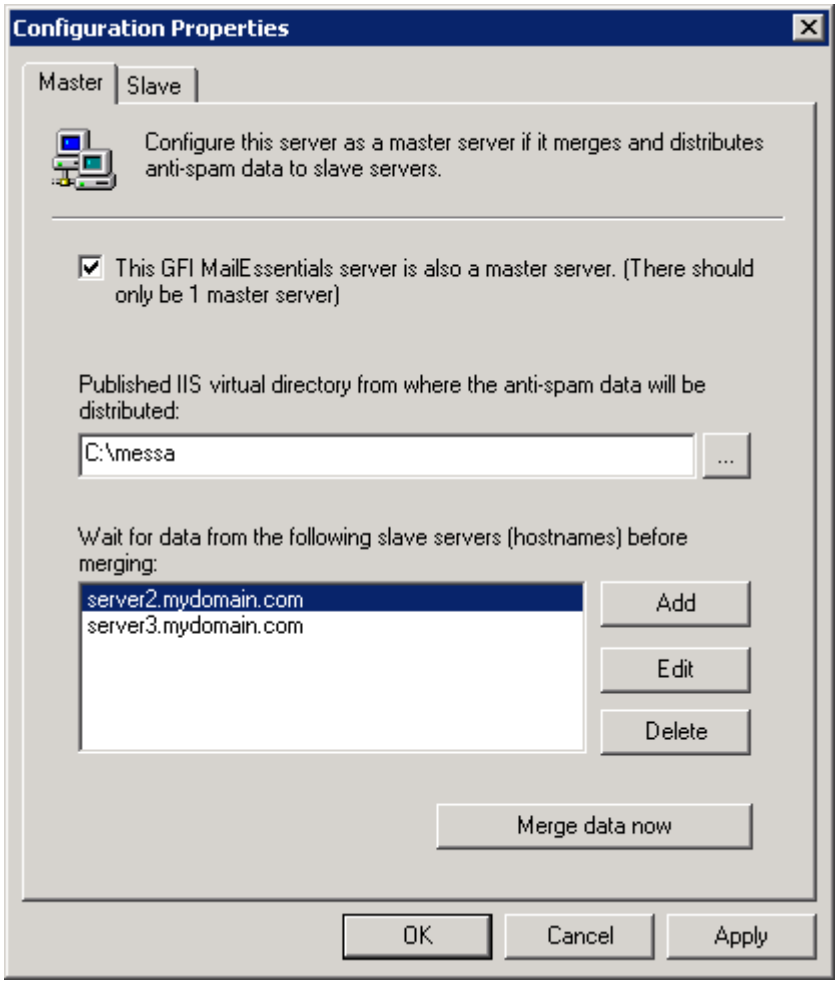
h. Click **OK**.

i. Select the **BITS Server Extension** tab and check **Allow clients to transfer data to this virtual directory** checkbox.

j. Click **OK** to close the virtual directory dialog properties.

8.2.3 Step 2: Configure the master server

1. Select **Start ► GFI MailEssentials ► GFI MailEssentials Anti-Spam Synchronization Agent**, right click **Anti-Spam Synchronization Agent ► Configuration** node and select **Properties**.


Configuration Properties
Master
Slave
Configure this server as a master server if it merges and distributes anti-spam data to slave servers.
This GFI MailEssentials server is also a master server. (There should only be 1 master server)
Published IIS virtual directory from where the anti-spam data will be distributed:
C:\messa
...
Wait for data from the following slave servers (hostnames) before merging:
server2.mydomain.com
server3.mydomain.com
Add
Edit
Delete
Merge data now
OK
Cancel
Apply

Screenshot 84 - Configuring a master server

2. From the **Master** tab, select **This GFI MailEssentials server is also a master server** checkbox and key in the full path of the folder configured to hold the contents of the **MESynchAgent** virtual directory.

3. Click **Add** button and enter the hostname of the slave server in the **Server** edit box. Click **OK** to add it to the list. Repeat this step and add all the other slave servers configured.

NOTE 1: Ensure that you configure all the machines you add to this list as slave servers, else the anti-spam synchronization agent on the master server will never merge the data.

NOTE 2: A master server can also be a slave server at the same time. In this case the server will merge its own anti-spam settings data to the ones uploaded by the other slave servers. For this to work it is required to add the master server hostname to the list of slave servers as well. For more information, refer to the **Step 3: Configure slave servers** section in this manual.

4. If required, select a slave server from the list and click the **Edit** or **Delete** button to edit or delete it.

5. Click the **OK** button to save the settings.

8.2.4 Step 3: Configure slave servers

Important notes

1. To configure a server as a slave server, it must meet one of the following system specifications:

- Microsoft Windows Server 2008
- Microsoft Windows Server 2003 - It is recommend that you download the BITS 2.0 client update from the following Microsoft link:

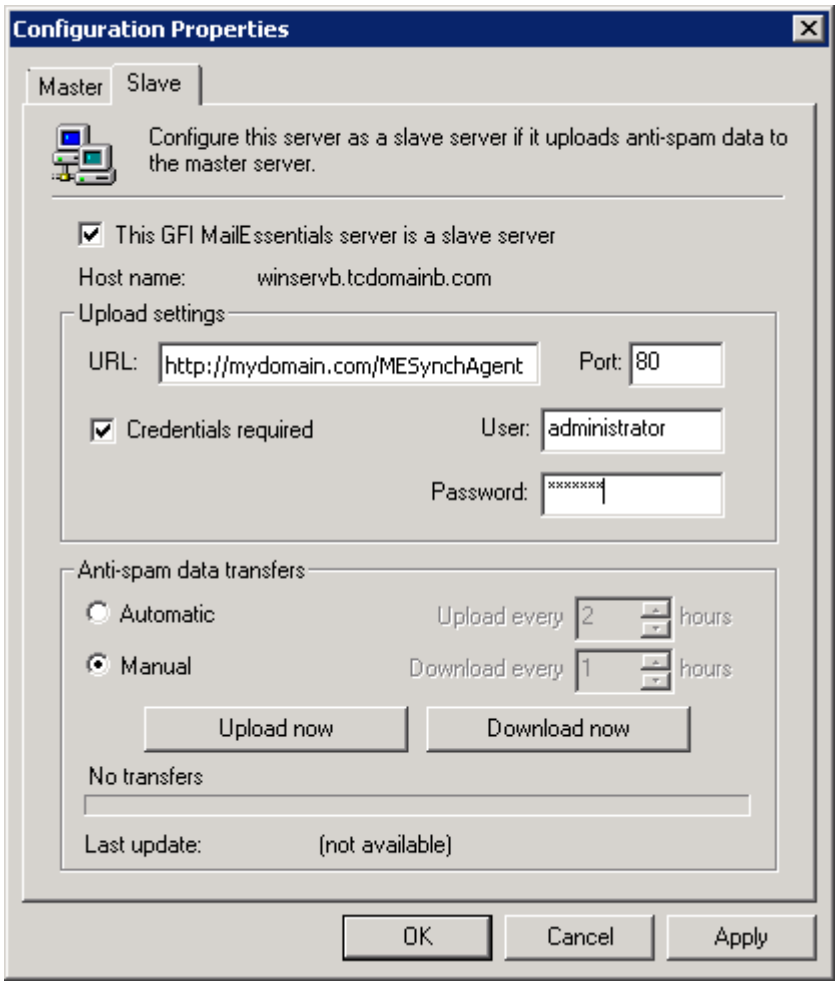
  http://www.microsoft.com/downloads/details.aspx?familyid=3FD31F05-D091-49B3-8A80-BF9B83261372&displaylang=en

2. Slave servers automatically upload an archive file, containing anti-spam settings to the IIS virtual directory on the master server, so no virtual directory should be created on slave servers.

Slave server configuration

1. Click **Start ► GFI MailEssentials ► GFI MailEssentials Anti-Spam Synchronization Agent**.

2. Right click **Anti-Spam Synchronization Agent ► Configuration** node and select **Properties**.



Screenshot 85 - Configuring a slave server

3. From the **Slave** tab, select **This GFI MailEssentials server is a slave server** checkbox.

4. In the **URL** field, specify the full URL to the virtual directory hosted on the master server in the following format:

```
http://<master server domain name>/MESynchAgent
```

- **Example:** `http://mydomain.com/MESynchAgent`

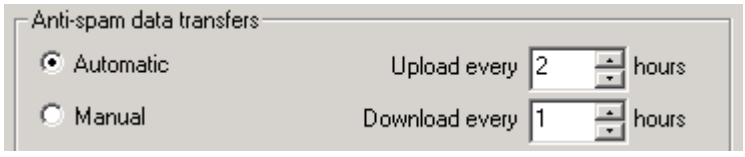
5. In the **Port** field specify the port used by the master server to accept HTTP communications.

NOTE: By default it is set to port 80 which is the standard port used for HTTP.

6. Check **Credentials required** checkbox and key in the username/password used to authenticate with the master server.

7. Select:

- **Manual -** Upload and download the anti-spam settings archive file manually. To upload the anti-spam settings of the slave server to the master server click **Upload now** button. To download the updated merged anti-spam settings from the master server, click **Download now** button.



Screenshot 86 - Upload / download hourly interval setting

- **Automatic -** Configures the anti-spam synchronization to occur automatically. In the **Upload every** field specify the upload interval in hours that determines how often the slave server will upload its anti-spam settings to the master server. In the **Download every**

field specify the download interval in hours which determines how often the slave server checks for updates on the master server and downloads them.

NOTE: The hourly interval for upload and download cannot be set to the same value. The hourly interval can be set to any value between 1 and 240 hours. It is recommended that the download interval is configured to a smaller value than the upload interval and that the same interval settings for all the slave servers are set for all slave servers configured.

- **Example:** If the download interval is set to 3 hours and the upload interval is set to 4 hours. This way downloads are more frequent than uploads.

8. Click the **OK** button to save the settings.

8.3 Exporting and importing GFI MailEssentials settings

GFI MailEssentials includes a Configuration Export/Import tool so that settings can be exported to other GFI MailEssentials installations.

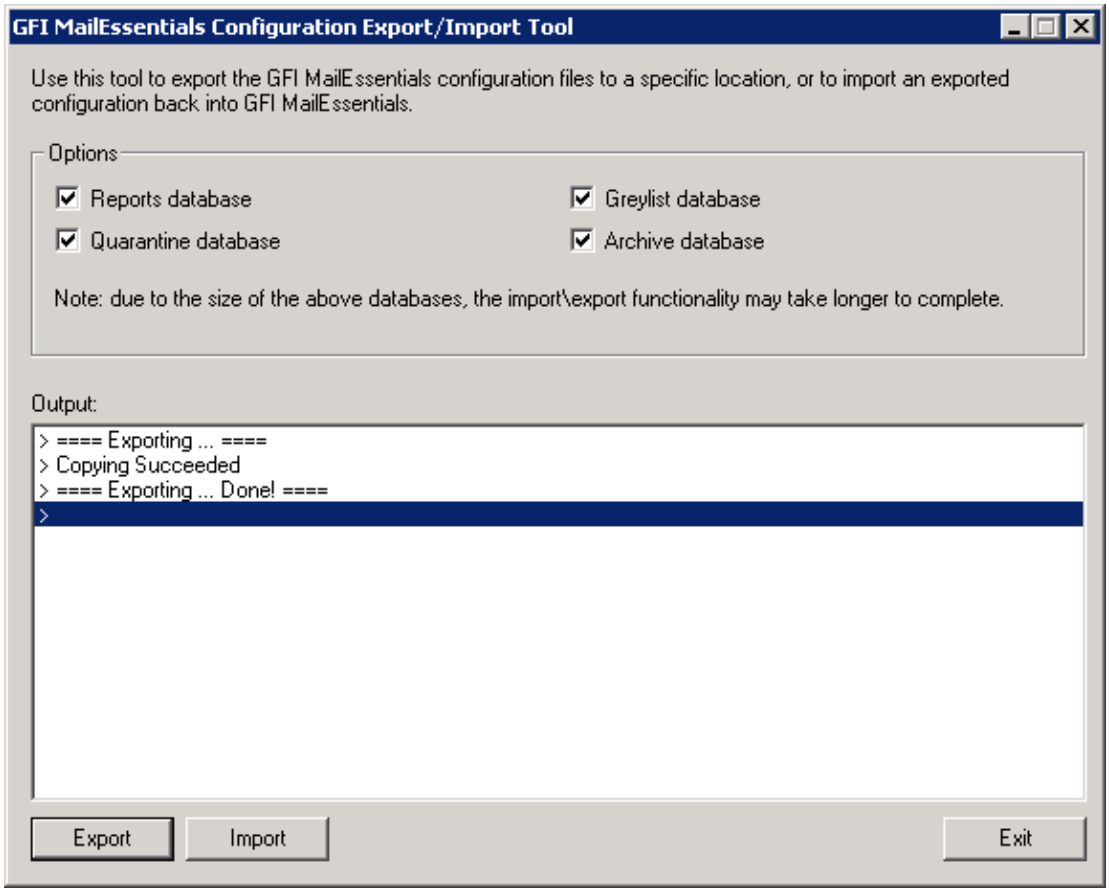
8.3.1 Step 1: Export existing GFI MailEssentials configuration settings

GFI MailEssentials provides two methods of exporting configuration settings:

- **Exporting via user interface**
- **Exporting settings via the command line**

Exporting via user interface

1. Stop the following GFI MailEssentials services:
   - GFI MailEssentials Scan Engine
   - GFI MailEssentials Managed Attendant Service
2. Navigate to the GFI MailEssentials root folder and launch **meconfigmgr.exe**.


GFI MailEssentials Configuration Export/Import Tool
Use this tool to export the GFI MailEssentials configuration files to a specific location, or to import an exported configuration back into GFI MailEssentials.
Options
Reports database
Greylist database
Quarantine database
Archive database
Note: due to the size of the above databases, the import\export functionality may take longer to complete.
Output:
> ==== Exporting ... ====
> Copying Succeeded
> ==== Exporting ... Done! ====
>
Export
Import
Exit

Screenshot 87 - GFI MailEssentials Configuration Export/Import Tool

3. (Optional) Apart from exporting the configuration settings, GFI MailEssentials allows export of other databases. Select the databases to export:

- Reports database
- Quarantine database
- Greylist database
- Archive database

NOTE: Duration of the export process depends on the databases' sizes.

4. Click **Export** button. In the **Browse for Folder** dialog choose a folder to export the GFI MailEssentials configuration settings and click **OK**.

5. On completion, click the **Exit** button.

6. Restart the services that were stopped in step 1.

Exporting settings via the command line

1. Stop the following GFI MailEssentials services:

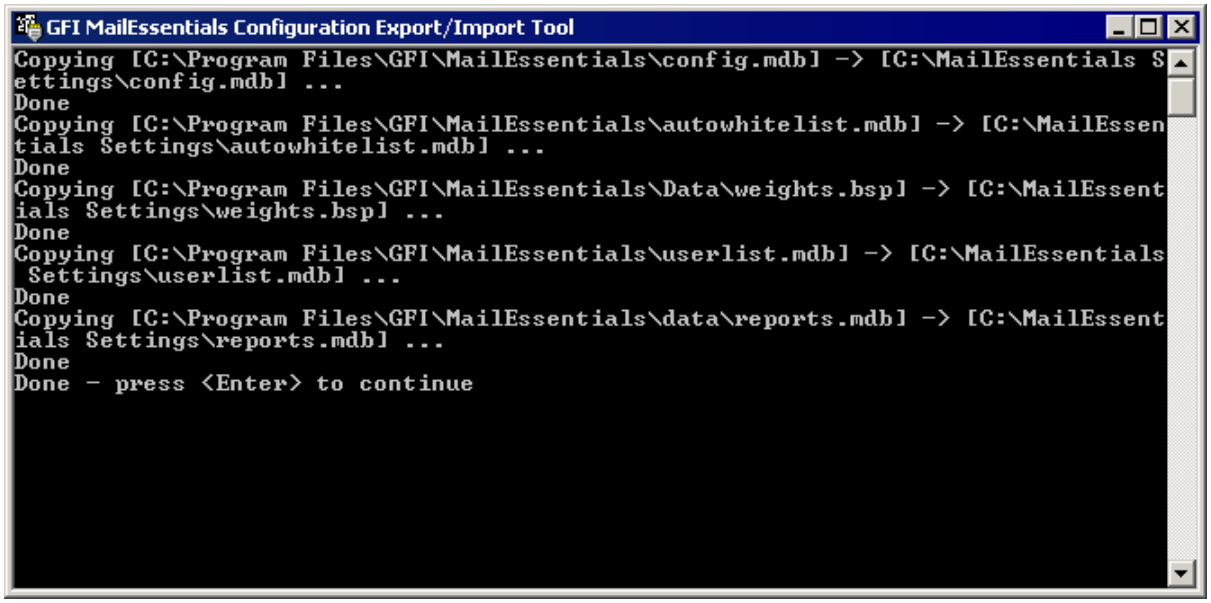
- GFI MailEssentials Scan Engine
- GFI MailEssentials Managed Attendant Service

2. From the command prompt, browse to the GFI MailEssentials installation root folder.

3. Key in:

```
meconfigmgr /export:"c:\MailEssentials Settings" /verbose /replace
```

NOTE: Replace "C:\MailEssentials Settings" with the desired destination path.


GFI MailEssentials Configuration Export/Import Tool
Copying [C:\Program Files\GFI\MailEssentials\config.mdb] -> [C:\MailEssentials Settings\config.mdb] ...
Done
Copying [C:\Program Files\GFI\MailEssentials\autowhitelist.mdb] -> [C:\MailEssentials Settings\autowhitelist.mdb] ...
Done
Copying [C:\Program Files\GFI\MailEssentials\Data\weights.bsp] -> [C:\MailEssentials Settings\weights.bsp] ...
Done
Copying [C:\Program Files\GFI\MailEssentials\userlist.mdb] -> [C:\MailEssentials Settings\userlist.mdb] ...
Done
Copying [C:\Program Files\GFI\MailEssentials\data\reports.mdb] -> [C:\MailEssentials Settings\reports.mdb] ...
Done
Done - press <Enter> to continue

Screenshot 88 - Exporting settings via command line

- The /verbose switch instructs the tool to display progress while copying the files.
- The /replace switch instructs the tool to overwrite existing files in the destination folder.

4. Restart the services that were stopped in step 1.

8.3.2 Step 2: Copy the exported settings

1. Manually copy the folder where the configuration settings were exported.

2. Paste the folder to the machines where to import the settings.

8.3.3 Step 3: Import settings to new GFI MailEssentials installation

GFI MailEssentials provides two methods of importing configuration settings:

- Importing via user interface
- Importing via the command line

IMPORTANT: When importing settings, the imported files overwrite existing GFI MailEssentials settings and may require reconfiguration of particular network settings and spam actions.

Importing via user interface

1. Stop the following services:

- GFI List Server
- GFI MailEssentials Enterprise Transfer Service
- GFI MailEssentials Legacy Attendant Service
- GFI MailEssentials Managed Attendant Service
- GFI MailEssentials Scan Engine
- GFI POP2Exchange
- IIS Admin service

2. Navigate to the GFI MailEssentials root folder and launch **meconfigmgr.exe**.

3. (Optional) Apart from importing the configuration settings, GFI MailEssentials allows import of other databases. Select the databases to import:

- Reports database
- Quarantine database
- Greylist database
- Archive database

NOTE: Duration of the import process depends on the databases' sizes.

4. Click **Import** button, choose the folder which contains the GFI MailEssentials import data and click **OK**.

WARNING: The import process replaces the installation files with the files found in this folder.

5. Imported settings may not be compatible with the installation of GFI MailEssentials and some settings may need to be re-configured. This is possible when certain network parameters (such as DNS settings, domains list and perimeter servers) are different from the server from which settings were exported. It is recommended to click **Yes** to launch the GFI MailEssentials Post-Installation wizard to reconfigure important settings. For more information about the steps in the Post-Installation wizard refer to the GFI MailEssentials Getting Started Guide available from http://www.gfi.com/mes/manual.

NOTE: For more information about settings to verify after import refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID003956.

6. On completion, click **Exit** button.

7. Restart the services that were stopped in step 1.

Importing via the command line

1. Stop the following services:

- GFI List Server
- GFI MailEssentials Enterprise Transfer Service
- GFI MailEssentials Legacy Attendant Service
- GFI MailEssentials Managed Attendant Service

- GFI MailEssentials Scan Engine
- GFI POP2Exchange
- IIS Admin service

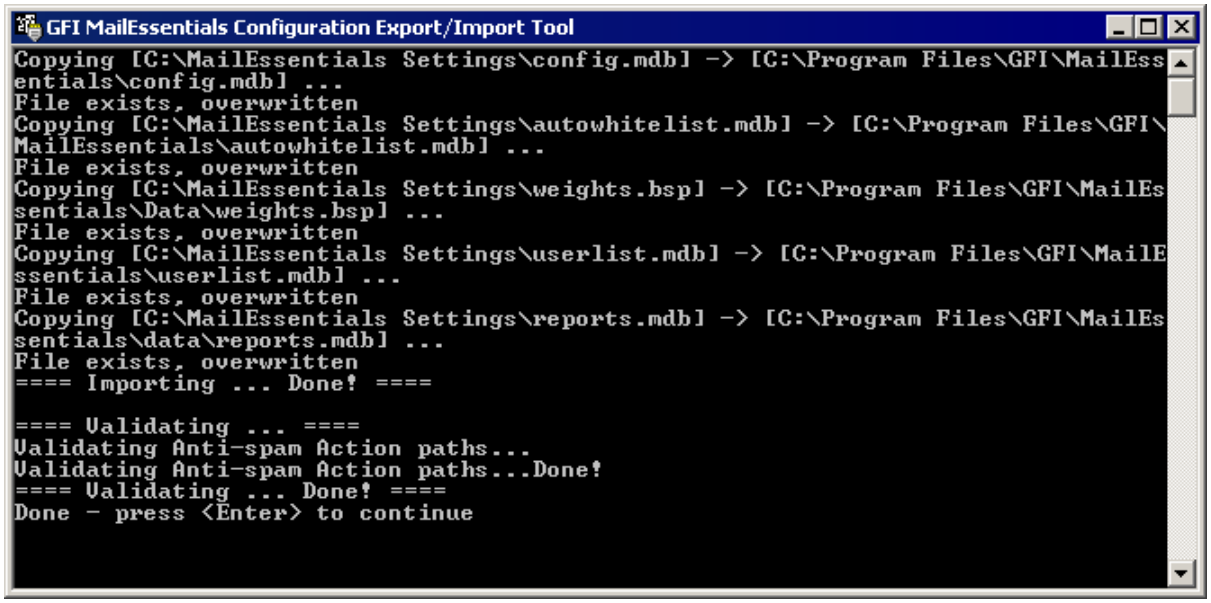
2. From a command prompt, browse to the GFI MailEssentials installation root folder.

3. Key in:

```
meconfigmgr /import:"c:\MailEssentials Settings" /verbose /replace
```

Note: Replace "C:\MailEssentials Settings" with the desired source path.

WARNING: The import process replaces the installation files with the files found in this folder.


GFI MailEssentials Configuration Export/Import Tool
Copying [C:\MailEssentials Settings\config.mdb] -> [C:\Program Files\GFI\MailEss
entials\config.mdb] ...
File exists, overwritten
Copying [C:\MailEssentials Settings\autowhitelist.mdb] -> [C:\Program Files\GFI\
MailEssentials\autowhitelist.mdb] ...
File exists, overwritten
Copying [C:\MailEssentials Settings\weights.bsp] -> [C:\Program Files\GFI\MailEs
sentials\Data\weights.bsp] ...
File exists, overwritten
Copying [C:\MailEssentials Settings\userlist.mdb] -> [C:\Program Files\GFI\MailE
ssentials\userlist.mdb] ...
File exists, overwritten
Copying [C:\MailEssentials Settings\reports.mdb] -> [C:\Program Files\GFI\MailEs
sentials\data\reports.mdb] ...
File exists, overwritten
==== Importing ... Done! ====
==== Validating ... ====
Validating Anti-spam Action paths...
Validating Anti-spam Action paths...Done!
==== Validating ... Done! ====
Done - press <Enter> to continue

Screenshot 89 - Importing settings via command line

- The /verbose switch instructs the tool to display progress while copying files.
- The /replace switch instructs the tool to overwrite existing files in the destination folder.

4. Restart the services that were stopped in step 1.

NOTE: Imported settings may not be compatible with the installation of GFI MailEssentials and some settings may need to be re-configured. For more information refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID003956.

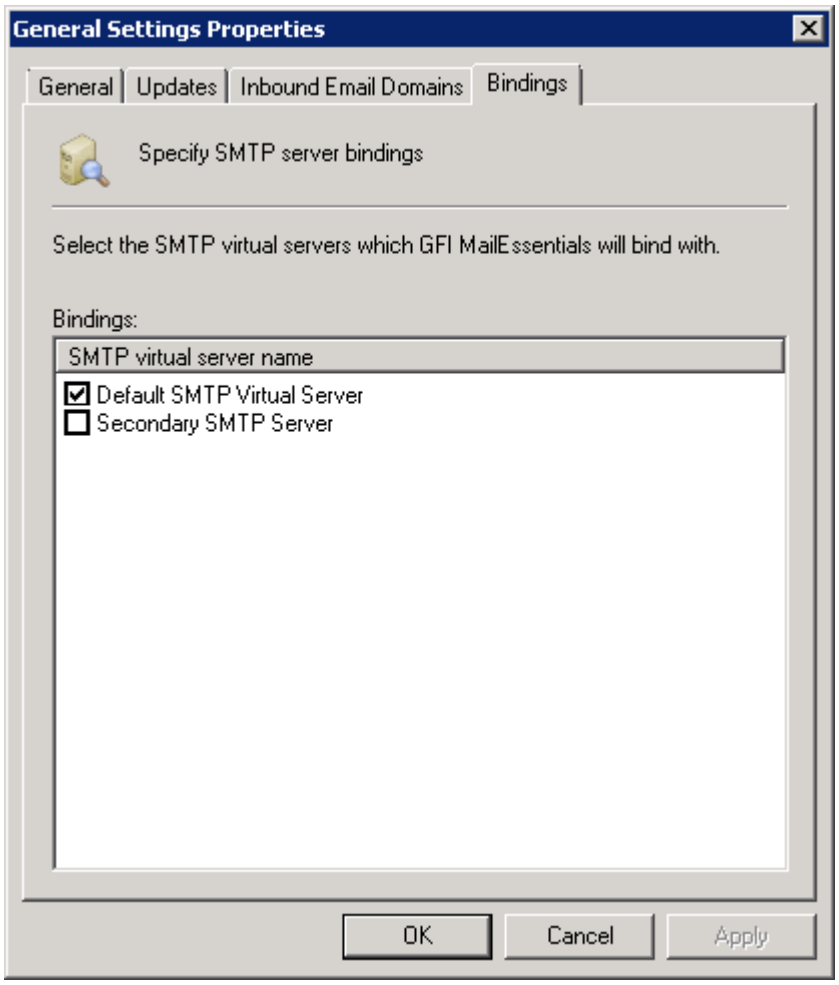
8.4 Selecting the SMTP Virtual Server to bind GFI MailEssentials

In case of multiple SMTP virtual servers, it might be required that GFI MailEssentials is bound to new or different SMTP Virtual Servers.

NOTE: The SMTP Virtual Server **Bindings** tab is not displayed if you installed GFI MailEssentials on a Microsoft Exchange Server 2007/2010 machine.

8.4.1 Binding GFI MailEssentials to SMTP Virtual Servers

1. Right click **General ► General Settings** node, select **Properties** and click **Bindings** tab.



Screenshot 90 - SMTP Virtual Server Bindings

2. From the **SMTP virtual server name** list, select the checkbox of the SMTP Virtual Server to bind GFI MailEssentials to.

3. Click **OK** button to finalize setup.

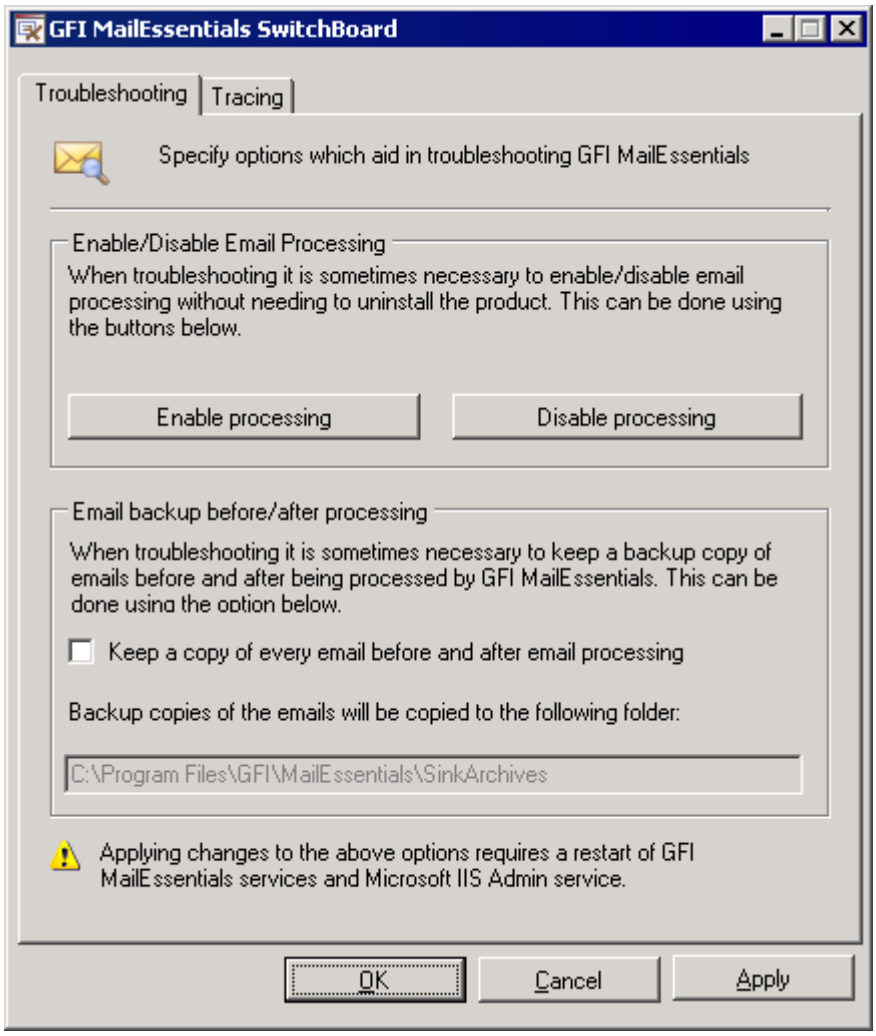
NOTE: The GFI MailEssentials configuration will ask to restart services such as the IIS SMTP Service for the new settings to take effect. Click **Yes** button to restart services.

8.5 Disabling/Enabling email processing

Disabling email processing disables all protection offered by GFI MailEssentials and enables all emails (including Spam) to get to your user's mailboxes.

To enable/disable GFI MailEssentials from processing emails:

1. Navigate to **Start ► Programs ► GFI MailEssentials ► GFI MailEssentials Switchboard**.


GFI MailEssentials SwitchBoard
Troubleshooting
Tracing
Specify options which aid in troubleshooting GFI MailEssentials
Enable/Disable Email Processing
When troubleshooting it is sometimes necessary to enable/disable email processing without needing to uninstall the product. This can be done using the buttons below.
Enable processing
Disable processing
Email backup before/after processing
When troubleshooting it is sometimes necessary to keep a backup copy of emails before and after being processed by GFI MailEssentials. This can be done using the option below.
Keep a copy of every email before and after email processing
Backup copies of the emails will be copied to the following folder:
C:\Program Files\GFI\MailEssentials\SinkArchives
Applying changes to the above options requires a restart of GFI MailEssentials services and Microsoft IIS Admin service.
OK
Cancel
Apply

Screenshot 91 - The GFI MailEssentials Switchboard: Troubleshooting

2. From the **Troubleshooting** tab click:

- » **Disable Processing** to disable email scanning
- » **Enable Processing** to enable email scanning

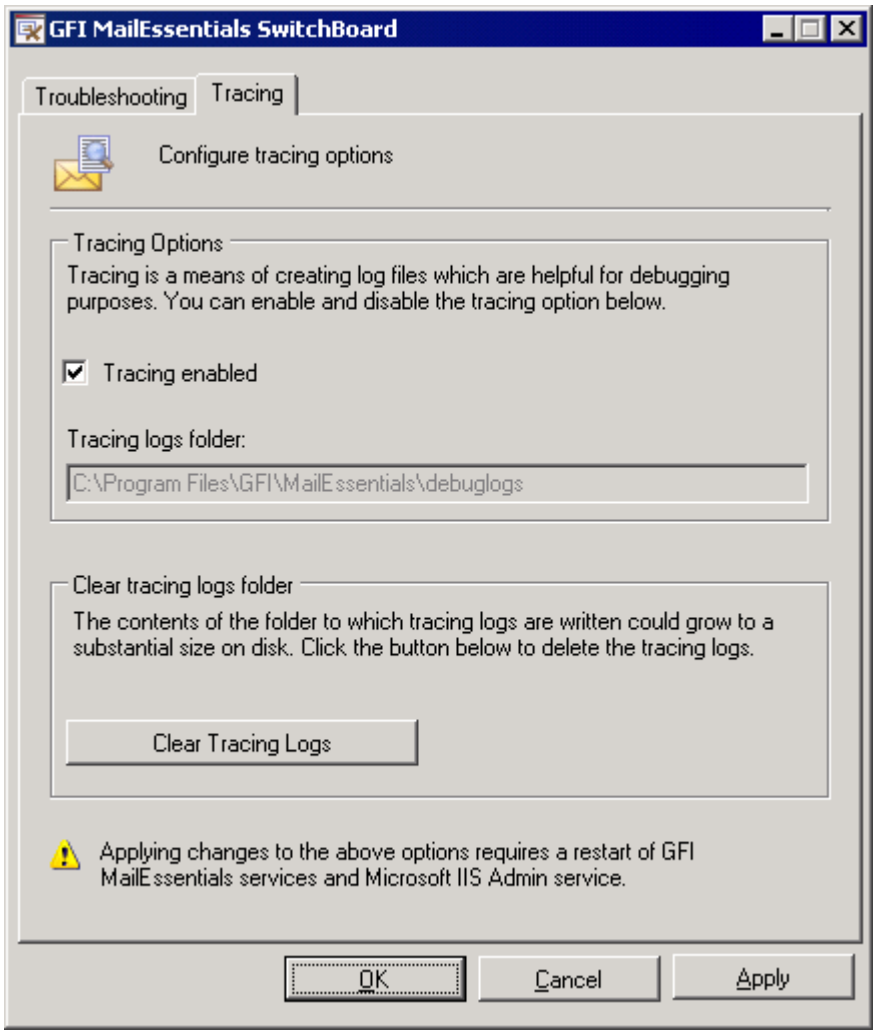
Email processing can be enabled/disabled through command prompt. For more information refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID003468.

8.6 Tracing

GFI MailEssentials can create logs for debugging purposes. When enabled, GFI MailEssentials stores logs in DebugLogs folder within the GFI MailEssentials installation folder. To configure Tracing:

1. Navigate to **Start ► GFI MailEssentials ► GFI MailEssentials Switchboard.**


GFI MailEssentials SwitchBoard
Troubleshooting
Tracing
Configure tracing options
Tracing Options
Tracing is a means of creating log files which are helpful for debugging purposes. You can enable and disable the tracing option below.
Tracing enabled
Tracing logs folder:
C:\Program Files\GFI\MailEssentials\debuglogs
Clear tracing logs folder
The contents of the folder to which tracing logs are written could grow to a substantial size on disk. Click the button below to delete the tracing logs.
Clear Tracing Logs
Applying changes to the above options requires a restart of GFI MailEssentials services and Microsoft IIS Admin service.
OK
Cancel
Apply

Screenshot 92 - Tracing

2. Select the **Tracing** tab and configure the following options:

- To enable/disable tracing, check/uncheck the **Tracing enabled** checkbox. This is enabled by default.
- Click **Clear Tracing Logs** to delete all logs

Email backup before and after processing

IMPORTANT: It is highly recommended that this option is left unchecked and used only for troubleshooting purposes under the recommendation of professional personnel.

From the **Troubleshooting** tab, check/uncheck the **Keep a copy of every email before and after email processing** checkbox to store a copy of each email processed in folder SinkArchives within the GFI MailEssentials installation folder.

8.7 Remote commands

Remote commands facilitate adding domains or email addresses to the Email Blocklist/Whitelist, as well as update the Bayesian filter with spam or ham (valid emails).

Remote commands work by sending an email to GFI MailEssentials. Addressing an email to rcommands@mailessentials.com (configurable) will have GFI MailEssentials recognize the email as containing remote commands and will process the commands.

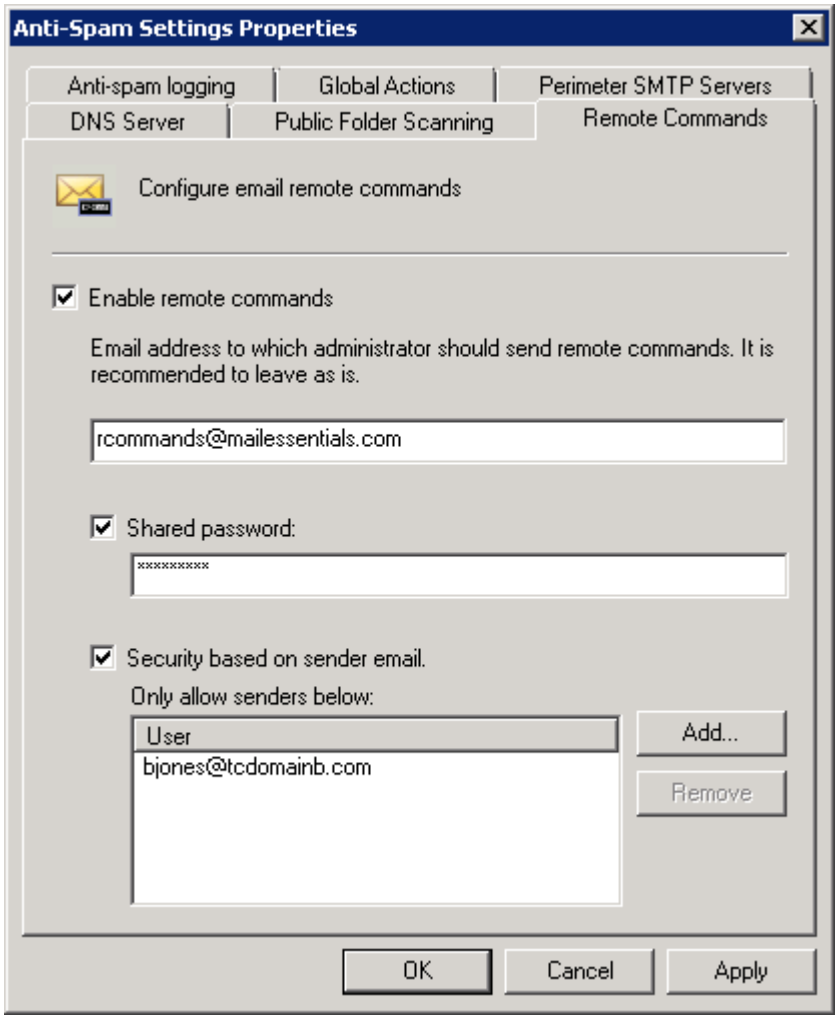
With remote commands, the following tasks can be achieved:

1. Add Spam or ham to the Bayesian module.

2. Add keywords either to the subject keyword checking feature or to the body keyword checking feature.

3. Add email addresses to the blocklist feature.

8.7.1 Configuring remote commands



Screenshot 93 - Remote commands configuration

1. Right click **Anti-Spam ► Anti-Spam Settings**, select **Properties**, click **Remote Commands** tab and check the **Enable remote commands** checkbox.

2. Edit the email address to which the remote commands should be sent.

NOTE: The email address should NOT be a local domain. It is recommended using rcommands@mailessentials.com. A mailbox for the configured address does not need to exist, but the domain-part of the address must consist of a real email address domain that returns a positive result to an MX-record lookup via DNS.

3. Optionally, configure some basic security for the remote commands:

- Configure a shared password to include in the email. For more information refer to **Using remote commands** section in this manual.
- Also configure which users are allowed to send emails with remote commands.

8.7.2 Using remote commands

Remote commands can be sent via email to GFI MailEssentials from an email client within the domain. Conditions for sending remote commands:

- The email must be in Plain Text format
- The subject of the email is ignored
- The following syntax must be used for all commands:

```
<command name>: <parameter1>, <parameter2>, <parameter3>, … ;
```

For example: `ADDSUBJECT: sex, porn, spam;`

- There can be more than one command in the body of an email with each command separated by a semi-colon (;).
- If a password is configured for remote commands, enter the password in the first line using the following syntax:

  `PASSWORD: <shared password>;`
- Command names are case-sensitive and should be written in UPPER CASE only.
- Conditions such as IF, AND, OR, … etc are not supported.
- Remote commands can only be used to add entries and not delete or modify existing entries.

8.7.3 Keyword commands

Use keyword commands to add keywords or combination of keywords in the body or subject lists in Keyword Checking filter.

Available commands are:

- **ADDSUBJECT** - Adds keywords specified to the subject keyword checking database.
  - **Example:** ADDSUBJECT: sex, porn, spam;
- **ADDBODY** - Adds keywords specified to the body keyword checking database.
  - **Example:** ADDBODY: free, “100% free”, “absolutely free”;

NOTE: When configuring phrases other than a single words, enclose phrases in double quotes (“ ”).

8.7.4 Blocklist commands

Using blocklist commands to add a single email address or an entire domain to the email blocklist.

Available commands are:

- **ADDBLIST:** <email>;
  - **Example:** ADDBLIST: user@somewhere.com;

NOTE 1: Add an entire domain to the blocklist by specifying a wildcard before the domain

- Example: ADDBLIST: *@domain.com.

NOTE 2: For security reasons, there can be only one ADDBLIST command in an email, and only one address can be specified as the command parameter. The parameter is either a user email or a domain:

- **Example:** spammer@spam.com or *@spammers.org.

NOTE 3: Wildcards cannot be used in domain names.

- Example: *@*.domain.com will be rejected as invalid.

8.7.5 Bayesian filter commands

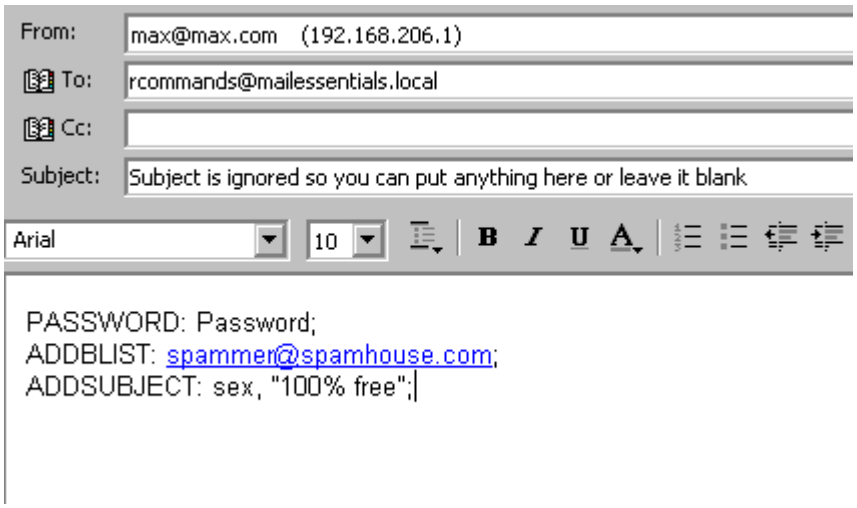
Add spam email or valid email (ham) to the Bayesian filter database. Available commands are:

- **ADDASSPAM** - instructs Bayesian filter to classify email as spam.
- **ADDASGOODMAIL** - instructs Bayesian filter to classify email as HAM.

NOTE: These commands do not have parameters - the rest of the email is the parameter.

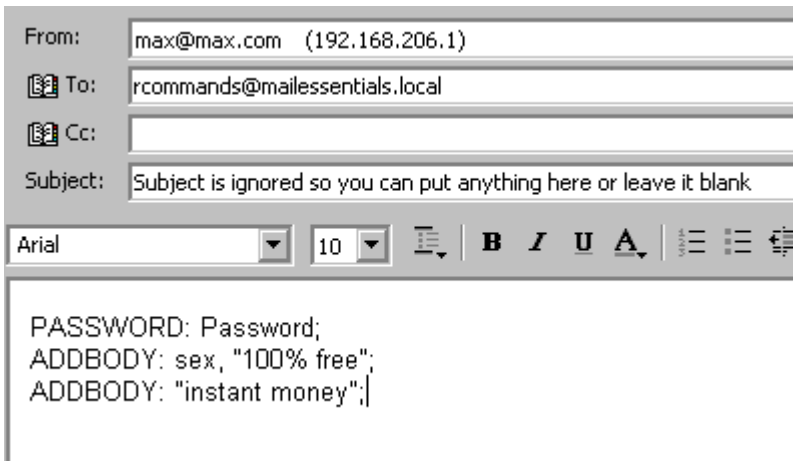
Examples

» **Example 1** - Through this example, the user adds spammer@spamhouse.com to the blocklist and add a few keywords to subject keyword checking database.



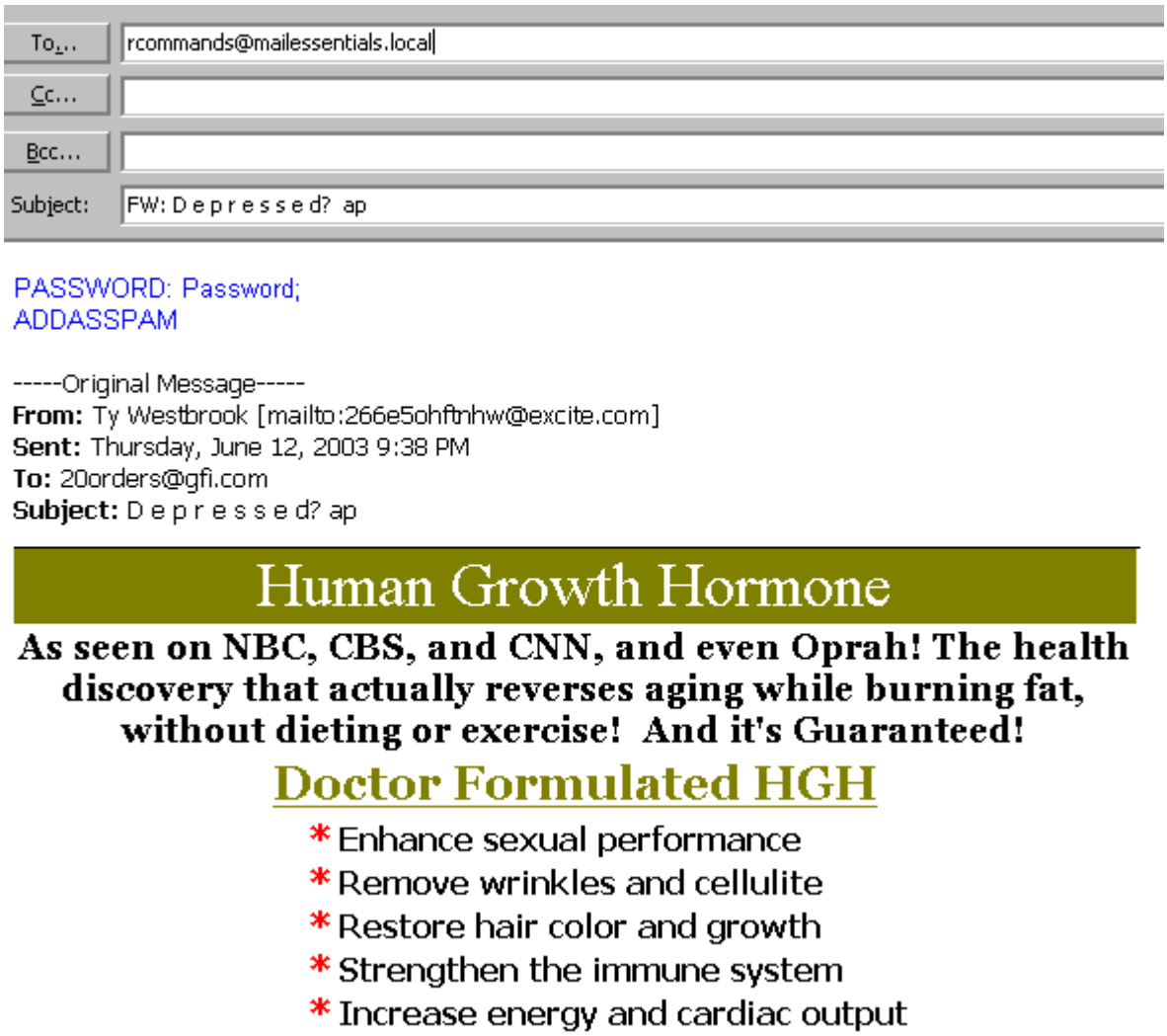
Screenshot 94 - Adding an email address to the blocklist and keywords

» **Example 2** - The same command can be specified more than once. (in this case ADDBODY). The result is cumulative, and in this case the keywords added to the body checking database are: sex, 100% free and instant money.



Screenshot 95 - Specifying the same commands more than once

» **Example 3:** A spam email is added using the ADDASSPAM command. A colon is not required for this type of command - everything immediately after this command is treated as data.


To...
rcommands@mailessentials.local
Cc...
Bcc...
Subject:
FW: D e p r e s s e d? ap
PASSWORD: Password;
ADDASSPAM
-----Original Message-----
From: Ty Westbrook [mailto:266e5ohftnhw@excite.com]
Sent: Thursday, June 12, 2003 9:38 PM
To: 20orders@gfi.com
Subject: D e p r e s s e d? ap
Human Growth Hormone
As seen on NBC, CBS, and CNN, and even Oprah! The health discovery that actually reverses aging while burning fat, without dieting or exercise! And it's Guaranteed!
Doctor Formulated HGH
* Enhance sexual performance
* Remove wrinkles and cellulite
* Restore hair color and growth
* Strengthen the immune system
* Increase energy and cardiac output

Screenshot 96 - Adding spam to the Bayesian filter database

» **Example 4** - When **Shared Password** checkbox is unchecked, remote commands can be sent without a password.

Screenshot 97 - Sending remote commands without security

8.7.6 Remote command logging

To keep track of changes made to the configuration database via remote commands, each email with remote commands (even if the email with remote commands was invalid) is saved under the ADBRProcessed subfolder located in GFI MailEssentials root folder. The file name of each email is formatted according to the following format:

» <sender_email_address>_SUCCESS_<timestamp>.eml - in case of successful processing.

» <sender_email_address>_FAILED_<timestamp>.eml - in case of failure.

NOTE: Timestamp is formatted as yyyyddmmhhmmss.

8.8 Moving spam email to user's mailbox folders

When GFI MailEssentials is installed on the Microsoft Exchange Server, spam emails can be saved in a user's mailbox folder as described in **Spam Actions - What to do with spam email** chapter of this manual.

If GFI MailEssentials is NOT installed on the Microsoft Exchange Server, spam emails cannot be routed to a specific user's mailbox folder through the Spam Actions. However, emails can still be routed to the user's mailbox as described below.

8.8.1 Microsoft Exchange Server 2003

GFI MailEssentials includes a Rules Manager utility that automatically moves emails tagged as spam to the users' mailbox.

IMPORTANT: To use the Rules Manager, in Spam Actions select the **Tag the email with specific text** option and specify a tag.

Install Rules Manager on the Microsoft Exchange Server

1. From the GFI MailEssentials machine, navigate to the GFI MailEssentials installation folder.

2. Copy the following files to a folder on the Microsoft Exchange Server:

- rulemgmtres.dll
- rulemgmt.exe
- rule.dll
- gfi_log.dll

3. From the Microsoft Exchange Server, open command prompt and change the directory to the location where the Rules Manager files were copied.

4. In command prompt type: **regsvr32 rule.dll**

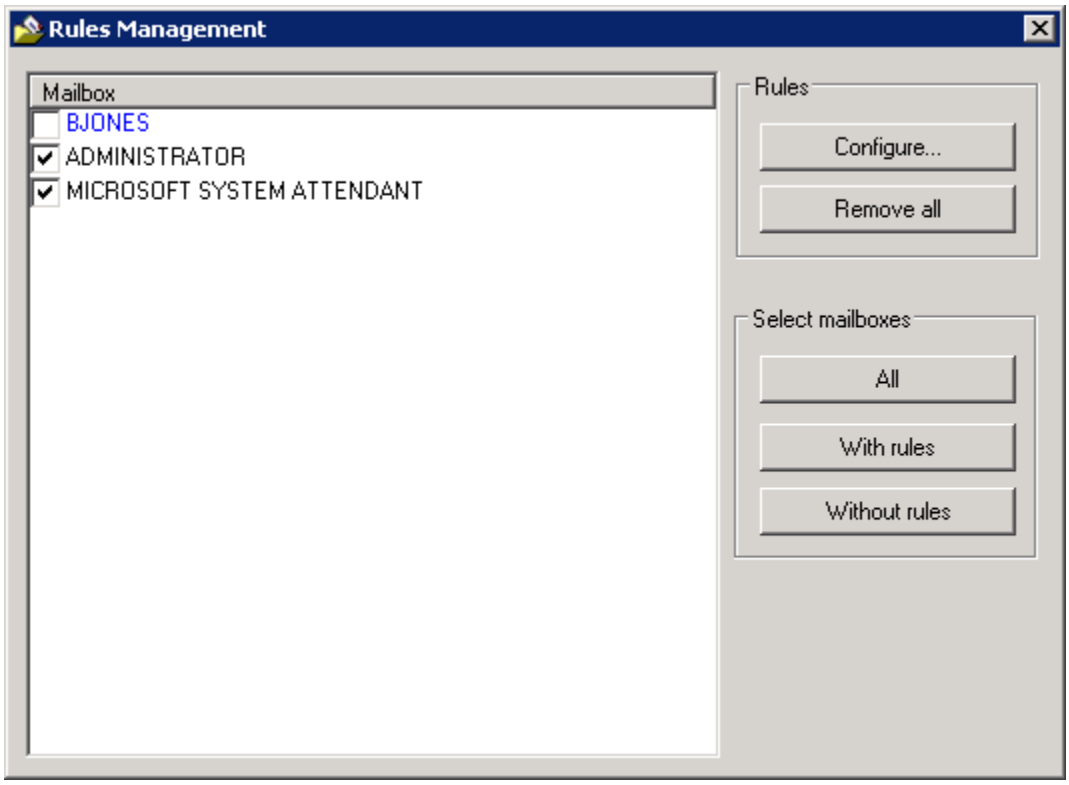
5. On confirmation, click **OK**.

Launch the Rules Manager

1. From the Microsoft Exchange Server, navigate to the location where the Rules Manager files were copied and open **rulemgmt.exe**.

2. Select a Microsoft Outlook profile (MAPI profile) or create a new profile to login (when using the Rules Manager the first time only).

3. Click **OK** to launch the Rules Manager.



Screenshot 98 - The GFI MailEssentials Rules Manager

4. The main window of the rules manager displays all the mailboxes enabled on the Microsoft Exchange Server. The color of the mailboxes indicates the status of that mailbox:

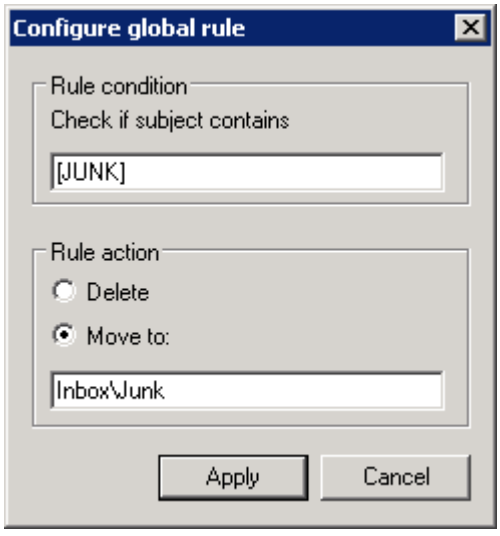
- Blue - mailbox has rules configured
- Black - mailbox has no rules configured.

Setting new rules

1. Check the mailboxes to set a rule on and click **Configure…** to launch the **Configure global rule** dialog.

NOTE 1: New rules can be added to mailboxes which already contain rules.

NOTE 2: Select multiple mailboxes to configure the same rule applicable to all mailboxes.



Screenshot 99 - Adding a new rule in Rules Manager

2. In the **Rule Condition** text box, type the tag given to the spam email in the GFI MailEssentials spam actions.

3. Specify the **Rule action**:

- Select **Delete** to delete an email which has a subject that contains the rule condition
- Select **Move to:** to move spam email to a folder in the mailbox. Key in the folder path where to save the spam email. If you specify **Inbox\Spam**, then a spam folder will be created in the Inbox folder. If you specify just **Spam**, then the folder will be created at the top level (same level as Inbox).

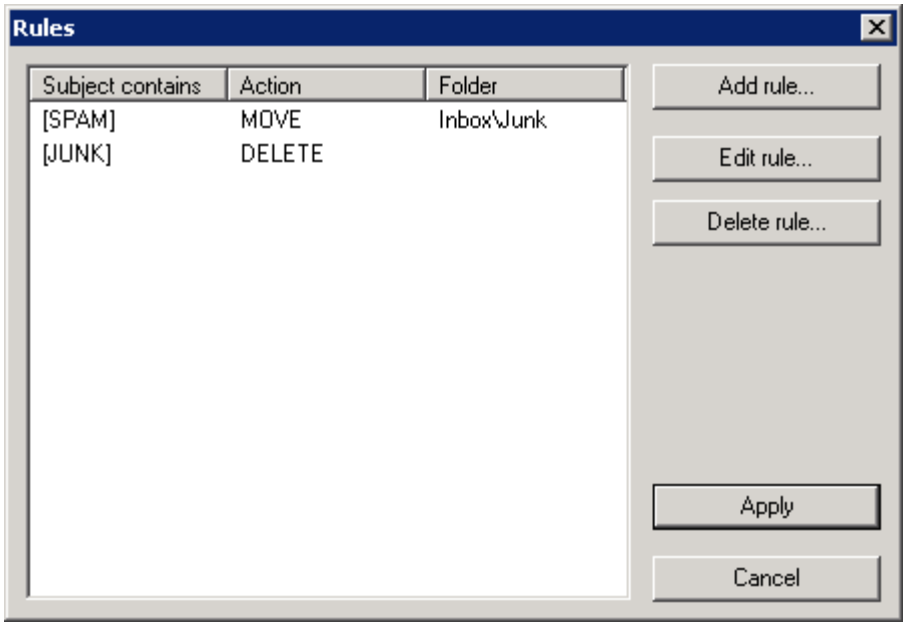
4. Click **Apply** to save the set rules.

Managing multiple rules

More than one rule can be set on the same mailbox.

Example: Delete emails tagged with [Phishing] and move emails tagged with [SPAM] to Inbox\Spam folder.

1. Double click on a mailbox to launch the Rules dialog.



Screenshot 100 - List of rules in Rules Manager

2. A list of rules applicable to the selected mailbox is displayed.
   - Click **Add rule** to add a new rule
   - Select a rule and click **Edit rule** to change settings of the selected rule
   - Select a rule and click **Delete rule** to delete the selected rule.
3. Click **Apply** to save settings.

8.8.2 Microsoft Exchange 2007/2010

To configure Microsoft Exchange 2007/2010 to forward tagged emails to the user's Junk E-mail mailbox folder, a Transport Rule needs to be created.

IMPORTANT: In GFI MailEssentials Spam Actions select the **Tag the email with specific text** option only. If you select any other action, the emails detected as spam will not reach the mailbox of the user, and therefore the configured transport rules will not be applicable.

To create a Transport Rule in Exchange 2007/2010:

1. Launch the **Microsoft Exchange Management Console**.

2. Navigate to **Microsoft Exchange ► Organization Configuration ► Hub Transport** and select the **Transport Rules** node.

3. Click on **New Transport Rule** to launch the wizard.

4. Type a name for the new rule (e.g. GFI MailEssentials SPAM) and click **Next**.

5. In the **Conditions** area select the option **When the Subject field contains specific words**.

6. In the **Edit rule** area, click **Specific Words** to enter the words used for tagging. Type the tag specified in the Spam Actions of each Spam filter and click **Add** (e.g. [SPAM]). Click **OK** when all words are added and click **Next**.

7. In the Actions area, select the option **Set the spam confidence level to value**.

8. In the **Edit rule** area, click **0** and set the confidence level to **9**. Click **OK** and click **Next**.

9. (Optional) Set any exceptions to this transport rule and click **Next**.

10. Click **New** to create the new Transport Rule.

NOTE: Ensure that the Junk E-Mail folder is enabled for the users' mailboxes.

The transport rule created will now forward all emails which contain the GFI MailEssentials tag to the users' Junk E-mail folder.

9 Troubleshooting & support

9.1 Introduction

This chapter explains how to resolve GFI MailEssentials issues encountered during installation. Use the following sources of information in the order listed below:

1. This manual
2. The common issues sections below
3. GFI Knowledge Base articles
4. Common checks
5. Web forums
6. Contacting GFI Technical Support

9.2 User manual

Use the information in this user manual to get an understanding of what might be causing any issues with your GFI MailEssentials installation. The information sections together with the common issues sections below will give you guidelines on what can be done to resolve any issues that might be due to misconfigurations or human error.

9.3 Common issues

The common issues listed below will enable you to investigate common issues encountered by users during their use of GFI MailEssentials.

9.4 Managing Spam

ISSUE ENCOUNTERED	SOLUTION
1. Dashboard shows no email is being processed; Or: Only inbound or outbound emails are being processed	1. Ensure that GFI MailEssentials is not disabled from scanning emails. For more information how to start scanning refer to **Disabling/Enabling email processing** section in this manual. 2. Check for multiple Microsoft IIS SMTP virtual servers and ensure that GFI MailEssentials is bound to the correct virtual server. 3. MX record for domain not configured correctly. Ensure that the MX record points to the IP address of the server running GFI MailEssentials 4. If inbound emails are passing through another gateway, ensure that the mail server running on the other gateway forwards inbound emails through GFI MailEssentials 5. Ensure that outbound emails are configured to route through GFI MailEssentials. Refer to installation manual for more details. 6. Verify that the SMTP virtual server used by Microsoft Exchange Server for outbound emails is the same SMTP server GFI MailEssentials is bound to. For more information how to solve this issue refer to: **http://kbase.gfi.com/showarticle.asp?id=KBID003286**
2. After installing GFI MailEssentials, some emails show a garbled message body when viewed in Microsoft Outlook	This problem occurs for emails that use one character set for the message header and a different character set for the message body. When such emails are processed by Microsoft Exchange 2003, the emails will be shown garbled in Microsoft Outlook. Microsoft has released a hotfix to resolve this issue. For more information how to solve this issue refer to: **http://kbase.gfi.com/showarticle.asp?id=KBID003459** and **http://support.microsoft.com/kb/916299**
3. Receiving spam emails from my	Some Spam emails contain a fake 'SMTP FROM' email address

ISSUE ENCOUNTERED	SOLUTION
domain.	consisting of the same domain as the recipient. This may seem as if the email is coming from a local user. 1. Configure the Sender Policy Framework filter to block emails originating from spoofed addresses. 2. Create an SPF record for your domain. For more information refer to http://kbase.gfi.com/showarticle.asp?id=KBID003567. 3. Ensure that 'Sender Policy Framework' module is configured to run at a higher priority than the Whitelist module. For more information refer to chapter Sorting anti-spam filters by priority.
4. Error when receiving emails: "Body type not supported by Remote Host"	This error occurs when emails are relayed from the IIS SMTP server to the Microsoft Exchange server. This happens because Microsoft Exchange Server versions 4.0, 5.0, and 5.5 are not able to handle 8-bit MIME messages. For instructions how to turn off 8BITMIME in Windows Server 2003 refer to: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q262168.
5. Processing of emails is very slow	This may occur when there are DNS problems in the network. If DNS is not working correctly, the DNS lookups made by some anti-spam filters in GFI MailEssentials will timeout. For more information refer to: http://kbase.gfi.com/showarticle.asp?id=KBID001770.

9.5 Archiving and Reporting

ISSUE ENCOUNTERED	SOLUTION
1. The **Mail Archiving** option is not available from the GFI MailEssentials configuration console.	Refer to http://kbase.gfi.com/showarticle.asp?id=KBID003989
2. AWI cannot be accessed with "HTTP Error 404 - File or directory not found" message	By default Internet Information Services (IIS) disables dynamic content. AWI requires this to be enabled, since data is dynamically retrieved from the archive database. 1. Load IIS Manager, expand **<Server Name> node ► Web service** extensions and right-click 'Active Server Pages'. 2. Click **Allow** to set status to 'Allowed'. For more information how to solve this issue refer to: http://kbase.gfi.com/showarticle.asp?id=KBID002963
3. Older data not available in database when using Microsoft Access.	When the reports.mdb database exceeds 1.7Gb, the database is automatically renamed to *reports_<data>.mdb* and a new reports.mdb is created. For more information how to solve this issue refer to: http://kbase.gfi.com/showarticle.asp?id=KBID003422

9.6 Anti-Spam filters & actions

ISSUE ENCOUNTERED	SOLUTION
1. Spam is delivered to users mailbox	Follow the checklist below to solve this issue: 1. Check that GFI MailEssentials is not disabled from scanning emails. Refer to **Disabling/Enabling email processing** in this manual for more information how to start scanning. 2. Check if all required anti-spam filters are enabled. 3. Check if local domains are configured correctly. 4. Check if emails are passing through GFI MailEssentials or if GFI MailEssentials is bound to the correct IIS SMTP Virtual Server. 5. Check if '%TEMP%' location (which by default is the 'C:\Windows\Temp' folder) contains a lot of files. 6. Check if the number of users using GFI MailEssentials exceeds the number of purchased licenses. 7. Check if whitelist is configured correctly. 8. Check if actions are configured correctly. 9. Check if Bayesian filter is configured correctly. For more information how to solve this issue refer to: **http://kbase.gfi.com/showarticle.asp?id=KBID003256**
2. Email Blocklist and/or Keyword Checking pages take long to load or appear to hang	Limit the amount of entries in the GFI MailEssentials lists to 10,000. For more information how to solve this issue refer to: **http://kbase.gfi.com/showarticle.asp?id=KBID002915** and: **http://kbase.gfi.com/showarticle.asp?id=KBID003267**
3. SpamRazer updates not downloading	1. Ensure that your license key is valid. 2. Ensure that the required ports are open and that your firewall is configured to allow connections from the GFI MailEssentials server to connect to any proxy server as defined in your configuration. For more information how to solve this issue refer to: **http://kbase.gfi.com/showarticle.asp?id=KBID002184**
4. Some spam emails bypass the Sender Policy Framework filter	As per the Sender Policy Framework standard, GFI MailEssentials Sender Policy Framework will only verify the 'SMTP From' header in an email and disregards the 'MIME From' header. A recent trend adopted by spammers is to use an 'SMTP From' address that does not have an SPF record. If GFI MailEssentials Sender Policy Framework has been configured on 'Low' or 'Medium', such emails will not be blocked by Sender Policy Framework as this does not result in an SPF fail. It is not recommended to set Sender Policy Framework to 'High' since the majority of mail servers do not yet have an SPF record. Such emails have a high chance of being blocked by SpamRazer or IP DNS Blocklists.
5. Emails are not being greylisted	To verify the operation of Greylist: Step 1: Confirm that Greylist is enabled » From the Greylist properties ensure that **Enable Greylist** is selected. Step 2: Verify excluded addresses » From the IP and Email exclusions in Greylist properties, ensure that there are no incorrect exclusions (such as **@*.com*). Step 3: Use esentutl.exe to ensure the Greylist database is not corrupted. For more information refer to: **http://kbase.gfi.com/showarticle.asp?id=KBID003463**

9.7 Quarantine

ISSUE ENCOUNTERED	SOLUTION
The Quarantine interface shows error D10 - "Cannot access the Quarantine Store database. Use a database repair tool (such as esentutl.exe) to repair the database."	Refer to http://kbase.gfi.com/showarticle.asp?id=KBID003463 for more information how to use esentutl.exe to repair the Quarantine Store database.

9.8 Disclaimers

ISSUE ENCOUNTERED	SOLUTION
1. No disclaimers are added to outbound emails	Disclaimers are only added to outbound emails originating from domains protected by GFI MailEssentials. Disclaimers are not added when: » Emails are sent from domains that are not specified in local domains list. » Emails are sent to domains which are incorrectly added in local domains list as these will be considered as internal emails. Ensure that all local domains are specified in the Inbound email domains dialog. For more information how to manage email domains refer to Inbound email domains section.
2. Some characters in disclaimer text are not displayed correctly	Configure Microsoft Outlook not to use automatic encoding and force GPO to use correct encoding. For more information how to solve this issue refer to: http://office.microsoft.com/en-us/ork2003/HA011402641033.aspx

9.9 Email monitoring

ISSUE ENCOUNTERED	SOLUTION
1. Emails sent from certain users, or sent to certain users are not monitored.	Email monitoring rules do not monitor emails sent from or to the GFI MailEssentials administrator and the email address to which the monitored emails are being sent to. Email monitoring rule also not available for emails sent between internal users of the same information store.

9.10 List Server

ISSUE ENCOUNTERED	SOLUTION
1. Emails sent to the list server are converted to Plain Text	Emails sent to the List server are converted to plain text emails only when the original format of the email is RTF. Send email in HTML format to retain original format
2. Internal users receive a non-delivery report when sending email to list server when GFI MailEssentials is installed on a Gateway machine	For more information how to use the List Server feature if GFI MailEssentials is installed on a gateway refer to: http://kbase.gfi.com/showarticle.asp?id=KBID002123

9.11 Miscellaneous

ISSUE ENCOUNTERED	SOLUTION
1. Clients connected to Microsoft Exchange via POP3 are not able to view mails blocked as SPAM	Connect to Microsoft Exchange using IMAP. For more information how to solve this issue refer to: http://kbase.gfi.com/showarticle.asp?id=KBID002644
2. Auto updates fail however manual download via the GFI MailEssentials configuration works fine	Ensure that un-authenticated connections are allowed from the GFI MailEssentials machine to http://update.gfi.com on port 80. For more information how to solve this issue refer to: http://kbase.gfi.com/showarticle.asp?id=KBID002116
3. Configuration data cannot be imported.	Ensure that the GFI MailEssentials version and build is identical across both source and target installations . For more information how to solve this issue refer to: http://kbase.gfi.com/showarticle.asp?id=KBID003182
4. Remote commands do not work	For information how to solve this issue refer to: http://kbase.gfi.com/showarticle.asp?id=KBID001806

9.12 Knowledge Base

GFI maintains a comprehensive Knowledge Base repository, which includes answers to the common user problems.

If the information in this manual does not help you solve your installation problems, next refer to the Knowledge Base. The Knowledge Base always has the most up-to-date listing of technical support questions and patches. Access the Knowledge Base by visiting:

http://kbase.gfi.com/

9.13 Common checks

If the information contained in this manual and the knowledge base repository do not help you solve your problems:

1. Ensure that all service packs for your operating system, mail server and GFI MailEssentials are installed.

2. Reinstall Microsoft Data Access Components (MDAC) to ensure its correct operation.

9.14 Web Forum

User to user technical support is available via the GFI web forum. After referring to the information in the user manual and in the knowledge base, access the web forum by visiting:

http://forums.gfi.com/.

9.15 Request technical support

If none of the resources listed above assist you in solving your issues, contact the GFI Technical Support team by filling in an online support request form or by phone.

- Online: Fill out the support request form and follow the instructions on this page closely to submit your support request on:

  http://support.gfi.com/supportrequestform.asp.

- Phone: To obtain the correct technical support phone number for your region please visit:

  http://www.gfi.com/company/contact.htm.

NOTE: Before contacting GFI's Technical Support, ensure to have your Customer ID available. Your Customer ID is the online account number that is assigned to you when you first register your license keys in our Customer Area at:

http://customers.gfi.com.

GFI endeavors to answer your query within 24 hours or less, depending on your time zone.

9.16 Build notifications

It is highly recommended that you subscribe to the build notifications list so that you are immediately notified about any new product builds. To subscribe to our build notifications, visit:

http://www.gfi.com/pages/productmailing.htm

9.17 Documentation

If this manual does not satisfy your expectations, or if you think that this documentation can be improved in any way, let us know via email on:

documentation@gfi.com

10 Appendix - Bayesian Filtering

The Bayesian filter is an anti-spam technology used within GFI MailEssentials. It is an adaptive technique based on artificial intelligence algorithms, hardened to withstand the widest range of spamming techniques available today.

This chapter explains how the Bayesian filter works, how it can be configured and how it can be trained.

NOTE: The Bayesian anti-spam filter is disabled by default. It is highly recommended that you train the Bayesian filter before enabling it.

IMPORTANT: GFI MailEssentials must operate for at least one week for the Bayesian filter to achieve its optimal performance. This is required because the Bayesian filter acquires its highest detection rate when it adapts to your email patterns.

How does the Bayesian spam filter work?

Bayesian filtering is based on the principle that most events are dependent and that the probability of an event occurring in the future can be inferred from the previous occurrences of that event.

NOTE: Refer to the links below for more information on the mathematical basis of Bayesian filtering:

http://www-ccrma.stanford.edu/~jos/bayes/Bayesian_Parameter_Estimation.html

http://www.niedermayer.ca/papers/bayesian/bayes.html

This same technique is used by GFI MailEssentials to identify and classify spam. The loci is that if a snippet of text frequently occurs in spam emails but not in legitimate emails, it would be reasonable to assume that this email is probably spam.

Creating a tailor-made Bayesian word database

Before Bayesian filtering is used, a database with words and tokens (for example $ sign, IP addresses and domains, etc,) must be created. This can be collected from a sample of spam email and valid email (referred to as 'ham').

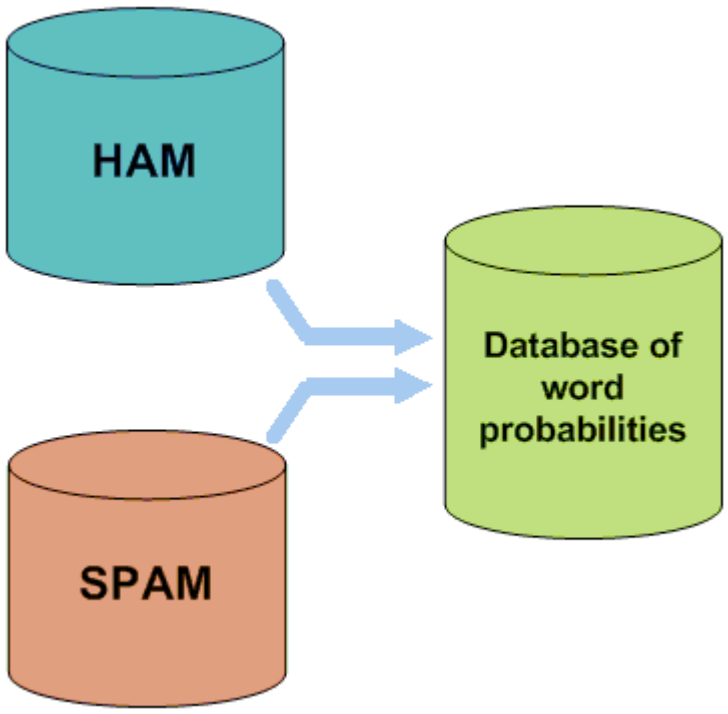


Figure 3 - Creating a word database for the filter

A probability value is then assigned to each word or token; this is based on calculations that account for how often such word occurs in spam as opposed to ham. This is done by analyzing the users' outbound email and known spam: All the words and tokens in both pools of email are

analyzed to generate the probability that a particular word points to the email being spam.

This probability is calculated as per following example:

If the word ‘mortgage’ occurs in 400 out of 3,000 spam emails and in 5 out of 300 legitimate emails then its spam probability would be 0.8889 (i.e. [400/3000] / [5/300 + 400/3000]).

Creating a custom ham email database

The analysis of ham email is performed on the company's email and therefore is tailored to that particular company.

- **Example:** A financial institution might use the word ‘mortgage’ many times and would get many false positives if using a general anti-spam rule set. On the other hand, the Bayesian filter, if tailored to your company through an initial training period, takes note of the company's valid outbound email (and recognizes ‘mortgage’ as being frequently used in legitimate messages), it will have a much better spam detection rate and a far lower false positive rate.

Creating the Bayesian spam database

Besides ham email, the Bayesian filter also relies on a spam data file. This spam data file must include a large sample of known spam. In addition it must also constantly be updated with the latest spam by the anti-spam software. This will ensure that the Bayesian filter is aware of the latest spam trends, resulting in a high spam detection rate.

How is Bayesian filtering done?

Once the ham and spam databases have been created, the word probabilities can be calculated and the filter is ready for use.

On arrival, the new email is broken down into words and the most relevant words (those that are most significant in identifying whether the email is spam or not) are identified. Using these words, the Bayesian filter calculates the probability of the new message being spam. If the probability is greater than a threshold, the message is classified as spam.

NOTE: For more information on Bayesian Filtering and its advantages refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID001813

10.1.1 Training the Bayesian Analysis filter

It is recommended that the Bayesian Analysis filter is trained through the organization’s mail flow over a period of time. It is also possible for Bayesian Analysis to be trained from emails sent or received before GFI MailEssentials is installed by using the Bayesian Analysis wizard. This allows Bayesian Analysis to be enabled immediately.

This wizard analyzes sources of:

- legitimate mail - for example a mailbox’ sent items folder
- spam mail - for example a mailbox folder dedicated to spam emails.

Step 1: Install the Bayesian Analysis wizard

The Bayesian Analysis wizard can be installed on:

- A machine that communicates with Microsoft Exchange - to analyze emails in a mailbox
- A machine with Microsoft Outlook installed - to analyze emails in Microsoft Outlook

1. Copy the Bayesian Analysis wizard setup file **bayesianwiz.exe** to the chosen machine. This is located in the **BSW** folder within the GFI MailEssentials installation folder

Example: C:\Program files\GFI\MailEssentials\BSW\bayesianwiz.exe

2. Launch **bayesianwiz.exe** and click **Next** in the welcome screen.

3. Select the installation folder and click **Next**.

4. Click **Next** to start installation.

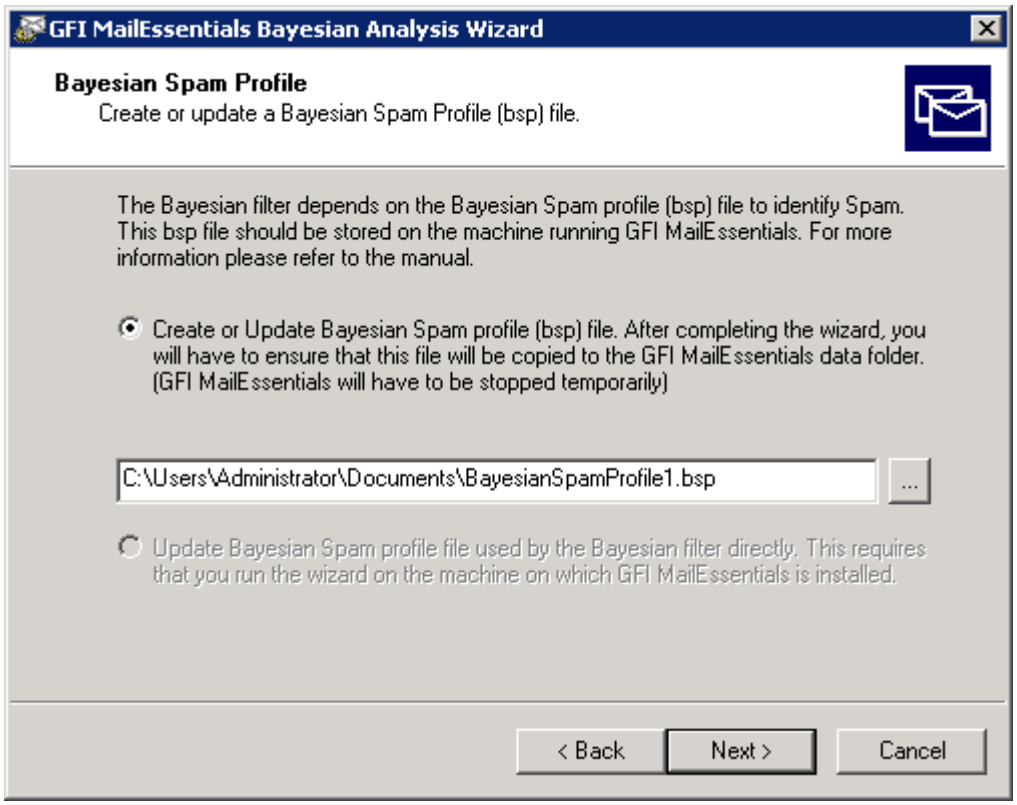
5. Click **Finish** when installation is complete.

Step 2: Analyze legitimate and spam emails

To start analyzing emails using the Bayesian Analysis wizard:

1. Load the Bayesian Analysis wizard from **Start ► Programs ► GFI MailEssentials ► GFI MailEssentials Bayesian Analysis Wizard**.

2. Click **Next** in the welcome screen.


GFI MailEssentials Bayesian Analysis Wizard
Bayesian Spam Profile
Create or update a Bayesian Spam Profile (bsp) file.
The Bayesian filter depends on the Bayesian Spam profile (bsp) file to identify Spam. This bsp file should be stored on the machine running GFI MailEssentials. For more information please refer to the manual.
Create or Update Bayesian Spam profile (bsp) file. After completing the wizard, you will have to ensure that this file will be copied to the GFI MailEssentials data folder. (GFI MailEssentials will have to be stopped temporarily)
C:\Users\Administrator\Documents\BayesianSpamProfile1.bsp
...
Update Bayesian Spam profile file used by the Bayesian filter directly. This requires that you run the wizard on the machine on which GFI MailEssentials is installed.
< Back
Next >
Cancel

Screenshot 101 - Select the Bayesian spam profile to update

3. Choose whether to:

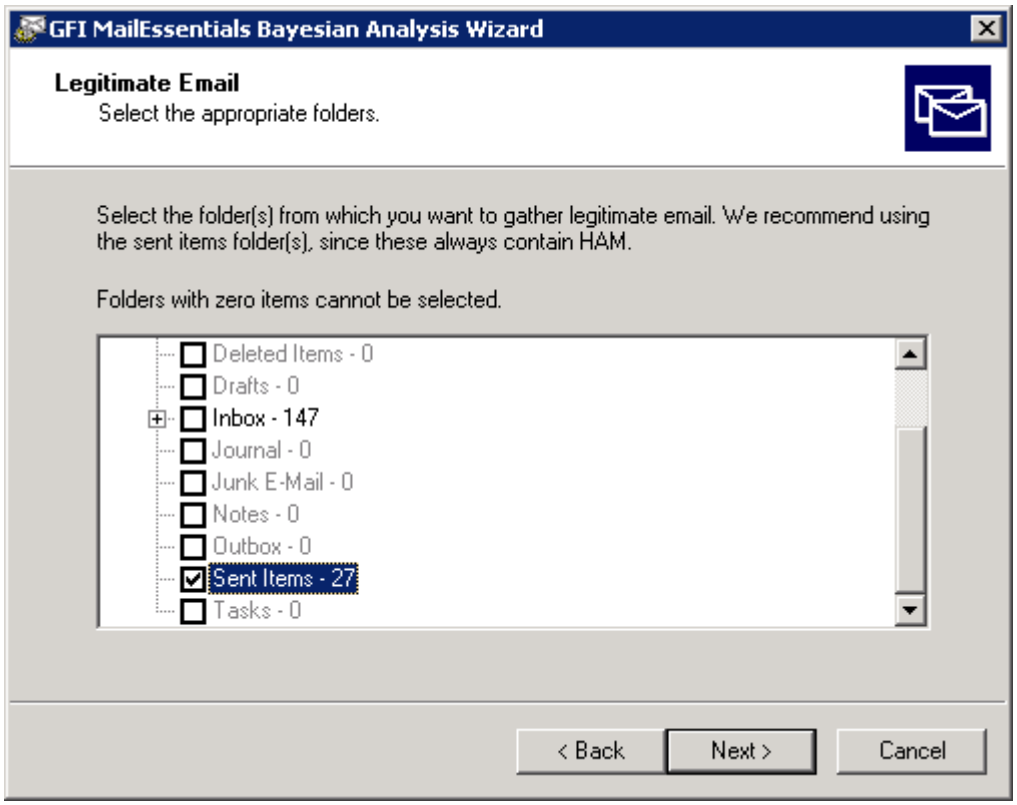
- Create a new Bayesian Spam Profile (.bsp) file or update an existing one. Specify the path where to store the file and the filename.
- Update the Bayesian Spam profile used by the Bayesian Analysis filter directly when installing on the same machine as GFI MailEssentials.

Click **Next** to proceed.

4. Select how the wizard will access legitimate emails. Select:

- **Use Microsoft Outlook profile configured on this machine** - Retrieves emails from a Microsoft Outlook mail folder. Microsoft Outlook must be running to use this option.
- **Connect to a Microsoft Exchange Server mailbox store** - Retrieves emails from a Microsoft Exchange mailbox. Specify the logon credentials in the next screen.
- Do not update legitimate mail (ham) in the Bayesian Spam profile - skip retrieval of legitimate emails. Skip to step 6.

Click **Next** to continue.


GFI MailEssentials Bayesian Analysis Wizard
Legitimate Email
Select the appropriate folders.
Select the folder(s) from which you want to gather legitimate email. We recommend using the sent items folder(s), since these always contain HAM.
Folders with zero items cannot be selected.
Deleted Items - 0
Drafts - 0
Inbox - 147
Journal - 0
Junk E-Mail - 0
Notes - 0
Outbox - 0
Sent Items - 27
Tasks - 0
< Back
Next >
Cancel

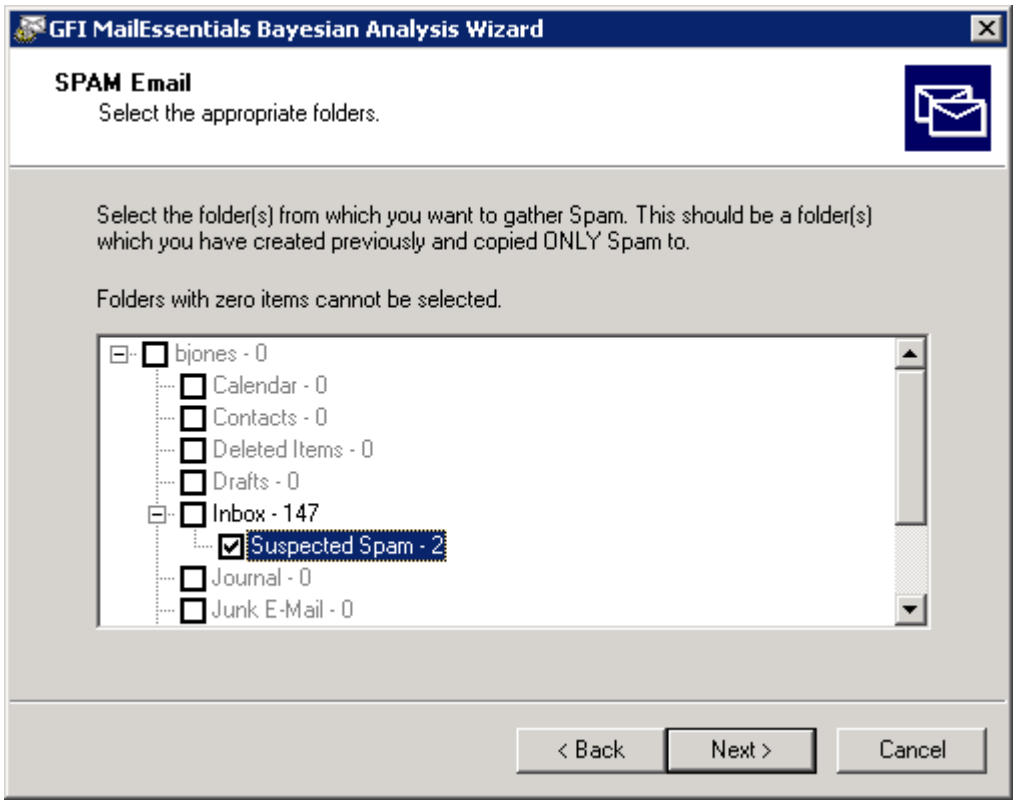
Screenshot 102 - Select the legitimate email source

5. After the wizard connects to the source, select the folder containing the list of legitimate emails (e.g. the Sent items folder) and click **Next**.

6. Select how the wizard will access the source of spam emails. Select:

- **Download latest Spam profile from GFI website** - Downloads a spam profile file that is regularly updated by collecting mail from leading spam archive sites. An internet connection is required.
- **Use Microsoft Outlook profile configured on this machine** - Retrieves spam from a Microsoft Outlook mail folder. Microsoft Outlook must be running to use this option.
- **Connect to a Microsoft Exchange Server mailbox store** - Retrieves spam from a Microsoft Exchange mailbox. Specify the logon credentials in the next screen.
- **Do not update Spam in the Bayesian Spam profile** - skip retrieval of spam emails. Skip to step 8.

Click **Next** to continue.


GFI MailEssentials Bayesian Analysis Wizard
SPAM Email
Select the appropriate folders.
Select the folder(s) from which you want to gather Spam. This should be a folder(s) which you have created previously and copied ONLY Spam to.
Folders with zero items cannot be selected.
bjones - 0
Calendar - 0
Contacts - 0
Deleted Items - 0
Drafts - 0
Inbox - 147
Suspected Spam - 2
Journal - 0
Junk E-Mail - 0
< Back
Next >
Cancel

Screenshot 103 - Select the spam source

7. After the wizard connects to the source, select the folder containing the list of spam emails and click **Next**.

8. Click **Next** to start retrieving the sources specified. This process may take several minutes to complete.

9. Click **Finish** to close the wizard.

Step 3: Import the Bayesian Spam profile

When the wizard is not run on the GFI MailEssentials server, import the Bayesian Spam Profile (.bsp) file to GFI MailEssentials.

1. Move the file to the **Data** folder in the GFI MailEssentials installation path.

2. Restart the GFI MailEssentials Scan Engine and the GFI MailEssentials Legacy Attendant services.

Index

A

Active Directory, 7, 40, 41, 66, 75, 81, 83, 84

Administrator email address, 100

Anti-spam actions, 13

Anti-spam global actions, 67

Anti-Spam Synchronization Agent, 108, 109, 110, 111

Auto Whitelist, 59, 60

Auto-replies, 7, 11, 85

B

Bayesian Analysis, 13, 55, 57, 136, 137

BITS server, 109

C

Configuration Export/Import Tool, 113

Custom footer, 90

D

Dashboard, 15, 16

Dialup downloading, 105

Directory harvesting, 11, 35, 39, 40, 41, 42

Disclaimers, 7, 81, 84, 85, 132

Discussion list, 34, 87, 91, 93

DMZ, 8, 40

DNS Server, 44, 52, 100, 101

E

Email Blocklist, 12, 35, 42, 61, 121

Email monitoring, 7, 11, 94, 95, 97, 132

Email processing, 11, 117, 118

Email routing, 99

Exchange 2003, 76

Exchange 2010, 66

F

Filter priority, 41

G

GFI MailEssentials reporter, 20

GFI MAX MailEdge, 102

GFI MAX MailProtection, 102

Greylist, 8, 13, 49, 51, 131

H

Header checking, 13, 51, 52

Hiding user posts, 76

I

IIS SMTP, 99, 129, 131

IMAP, 8, 73, 74, 78, 133

Inbound email domains, 99, 132

Inbound mail filtering, 11

Internal email, 41, 132

IP DNS Blocklist, 12, 44, 100, 131

IP Whitelist, 51, 61

J

Junk E-mail folder, 33, 127

K

Keyword checking, 7, 20, 54, 119, 121, 131

L

LDAP lookups, 40, 41

Legitimate email, 8, 33, 34, 41, 53, 56, 57, 135, 137, 138

Licensing, 14

List servers, 52, 87

Lotus Domino, 72, 77

M

Mail Monitoring, 7, 11, 94, 95, 97, 132

MAPI, 8, 73, 124

Microsoft Access, 19, 89, 130

Microsoft Exchange Server, 65, 66, 67, 73, 75, 94, 124, 129, 130, 138

Microsoft IIS, 69

Microsoft SQL Server, 19, 89

MSMQ, 9

N

New Senders, 11, 35, 61, 62, 63

Newsletter, 8, 87, 89, 91, 92, 93, 94

O

Outbound mail filtering, 12

P

perimeter server, 9

Phishing, 9, 12, 35, 37, 38, 39, 103

POP2Exchange, 9, 16, 105, 106

POP3, 7, 8, 9, 105, 106

Public folder scanning, 33, 72, 73, 78

Q

Quarantine, 7, 13, 29, 30, 31, 32, 33, 65, 68, 69, 70, 71, 72, 131

R

Remote commands, 9, 12, 119, 120, 121, 123

Reports, 7, 19, 20, 26, 27, 32, 70, 71, 130

Rules manager, 124, 125

S

Sender Policy Framework, 12, 46, 129, 131

SMTP Server, 44, 46, 49, 83, 101, 102, 130

SMTP transmission filtering, 41

SMTP Virtual Server, 116, 117, 129, 131

Spam actions, 9, 13, 64, 65, 124, 125, 127

Spam database, 34, 72, 136

SpamRazer, 12, 35, 36, 37, 64, 131

Statistics, 15, 20, 21, 22, 23, 24

T

Tag Email, 66

Tracing, 118, 119

U

Updates, 35, 37, 39, 57, 102, 103, 131

URI DNS Blocklist, 12, 45, 100

W

WebDAV, 9, 73, 74

Whitelist, 7, 12, 32, 33, 34, 35, 48, 51, 57, 58, 59, 60, 61, 63, 119, 131

USA, CANADA, CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

Email: ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

Email: sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

Email: sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

Email: sales@gfiap.com